Federal Policy towards Emergency Responder Interoperability: A Path Forward

by

Tristan Weir

Bachelor of Science
Arizona State University, 2004

Submitted to the Engineering Systems Division
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Technology and Policy

at the

Massachusetts Institute of Technology

June 2006

Signature of Author.....
Technology and Policy Program, Engineering Systems Division
May 12, 2006

Certified by.....
Lawrence McCray
Lecturer, Department of Political Science
Thesis Supervisor

Accepted by.....
Dava J. Newman
Professor of Aeronautics and Astronautics and Engineering Systems
Director, Technology and Policy Program

Federal Policy towards Emergency Responder Interoperability: A Path Forward

by

Tristan Weir

Submitted to the Engineering Systems Division on May 12, 2006
in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Technology and Policy

Abstract

Emergency responders have suffered from a lack of cross-agency radio communications for the past three decades. After numerous firefighters died in the terrorist attacks of September 11, partially due to a lack of interoperability with police officers on the scene, the federal government began implementing policies, programs, and funding to improve interoperability amongst state and local first responders. This thesi explores the scope and the effectiveness of many of the federal efforts towards interoperability that have occurred between 2001 and 2006.

Since 2001, the federal government has made progress in a number of areas relating to the national interoperability of first responders. These include: creating and reorganizing interoperability programs, such as SAFECOM within DHS; promoting open standards for equipment manufacturers; freeing radio spectrum for first responder use; and partially funding the purchase of new, interoperable communication equipment through grant programs and national initiatives. However, these efforts were slow to start, with the majority of progress only occurring within the past two years. Furthermore, the government has not set broad interoperability goals, and there are continuing questions about the amount of financial support that the government has offered and will continue to offer towards the problem. The European Union and the U.S. military have both dealt with interoperability as well, and comparisons between these two entities and the U.S. federal government show that a lack of interoperability is both complex and has some possible solutions that remain untested in the United States.

Five recommendations are presented to help the federal government forge a path forward. The government, through both the Department of Homeland Security and Congress, should: encourage collaboration between local public safety agencies; encourage better industry participation through equipment endorsements and public/private partnerships; create an interoperability grants program within DHS; prepare for a large increase in funding requests by 2009; and, establish a National Interoperability Goal with measurable results.

Thesis Supervisor: Lawrence McCray
Lecturer, Department of Political Science

Acknowledgements

First and foremost, I would like to thank my advisor, Dr. Larry McCray, for his patient and diligent help in developing this thesis. He challenged me to make this a product that I am truly proud of. I would also like to thank Dr. David Boyd, Dereck Orr, Vin Doherty, and Nelson Torres for agreeing to be interviewed. Their candor and insights were helpful beyond measure. Thanks to Juliette Kayyem and Lara Pierpoint, who provided comments that helped make this a better paper. Finally, special thanks to my parents, Maurice and Kerry, for giving me all the love and support in the world for the past 24 years.

Author Biography

Tristan Weir first became interested in homeland security issues as an undergraduate student at Arizona State University, while working towards a Bachelor of Science in Computer Science. In 2003, he received the Department of Homeland Security Scholarship and wrote his undergraduate thesis on the use of software middleware to enhance emergency responder capabilities. After graduating from ASU in 2004, he entered the Technology and Policy Program at MIT where he was funded by a Department of Homeland Security Fellowship. He has recently interned at both Sandia National Labs and the DHS Domestic Nuclear Detection Office.

This research was performed while on appointment as a U.S. Department of Homeland Security (DHS) Fellow under the DHS Scholarship and Fellowship Program, a program administered by the Oak Ridge Institute for Science and Education (ORISE) for DHS through an interagency agreement with the U.S Department of Energy (DOE). ORISE is managed by Oak Ridge Associated Universities under DOE contract number DE-AC05-06OR23100. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE, or ORISE.

Table of Contents

List of Figures

List of Tables

Chapter 1 – The Need for Interoperable Communications

April 19, 1995 – At 9:02 am, a truck bomb with over 4,000 pounds of explosives detonated outside the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. The front face and top floors of the building collapsed, over 800 people were injured, and 167 people were killed. Numerous state, local, and federal emergency responders quickly converged on the scene of the bombing, ready to move in and save lives. The Oklahoma City Fire Department, as well as surrounding area fire departments and FEMA search and rescue teams, began to scout the building for survivors. The Oklahoma City Police Department, the Oklahoma county sheriff, and Oklahoma National Guard units secured the perimeter around the building and assisted with the rescue efforts. The Emergency Medical Services Agency set up a triage center for helping the injured and getting serious cases to the local hospital. The FBI almost immediately began a criminal investigation of the bombing.

In the first hours of the response, communication between the dozen on-site agencies was problematic, at best. Fragmented communication frequencies and conflicting standards meant that police officers and firefighters could not use their radios to talk to one another or communicate with federal agencies. Cellular phone networks were quickly overloaded, and landline phones were impractical for responders moving throughout the destroyed building. Face-to-face communication and designated runners were used extensively to transmit messages, but these were inefficient and limited the flow of information to off-site incident commanders (Manzi, Powers, and Zeterlund

2002). In short, no system was available to efficiently and effectively allow the numerous response agencies to coordinate their life-saving efforts.

April 20, 1999 – Between 11:19 am and 12:05 pm, Eric Harris and Dylan Klebold, two gun-wielding sixteen-year-old students, went on a killing spree through Columbine High School in Littleton, Colorado. In the end, the two perpetrators killed themselves, but not before murdering 13 others and injuring dozens more. As in Oklahoma City, the emergency response was massive. Almost immediately following the first 911 call, a number of paramedics, firefighters and police officers arrived on scene. They were subsequently joined by almost 1,000 other responders including sheriff deputies, SWAT team members, medics and, later, FBI agents. Unlike the Oklahoma City bombing, however, the response was not just a search and rescue mission. Because it was unclear, until late in the afternoon, how many perpetrators were in the school and whether or not they were all dead, responders approached the school as if it still contained unknown threats. For much of that day, many of the emergency responders on the scene were anticipating further loss of life.

As the number of agencies on scene increased, so did the magnitude of the communication problems. Responding agencies from different jurisdictions were using incompatible communication equipment. Some systems were analog, while others were digital. Some used proprietary Motorola standards, while others used proprietary Ericsson standards. Almost all operated in isolated frequency bands. These incompatibilities "greatly increased the difficulty of establishing and maintaining effective incident command" and hampered the joint SWAT response as officers entered the building (Rosegrant and Howitt 2001). Said one Jefferson County Sheriff Officer, "I cannot

overemphasize how great a problem the incompatibility of our communications systems was that day. [It] was almost unimaginable" (Rosegrant and Howitt 2001).

September 11, 2001 – At 8:46 am, a fuel-laden jetliner piloted by al-Qaeda terrorists slammed into the middle of the north tower of the World Trade Center in New York City. At 9:03 am, a second terrorist-flown jetliner collided with the south tower. The force of the impacts eventually caused both towers to collapse, but not before New York Fire Department, New York Police Department, and New York/New Jersey Port Authority officers mounted a massive search and rescue operation in the Twin Towers.

On that tragic day, the firefighters, police officers, and Port Authority officers that struggled to evacuate the burning towers lacked the ability to talk to each other via radios. Their three separate communication systems were technically incompatible and operated on different frequencies. As a result, there was limited coordination between the three agencies during the evacuation. Areas that had been searched by firefighters were searched again by police. Rescue operations were conducted without knowledge or regard for nearby resources from other agencies. Most tragically, this lack of interoperable communication was at least partially responsible for the deaths of some of the roughly 200 firefighters that perished in the north tower, because they never received the message broadcasted on NYPD radio channels that the collapse of that tower was imminent (Kean, Hamilton, and et al. 2004).

August 29, 2005 – Hurricane Katrina, a Category 4 storm, ravaged the Gulf Coast and caused the levees surrounding New Orleans to break, flooding the city. This storm was exceptional, both in its ferocity and its lethality. The death toll from the hurricane and the subsequent flooding in Louisiana is estimated at 1,287, with most of those

fatalities occurring in and around New Orleans. While it is often criticized as being too little too late, there was a huge response by federal, state, and local emergency responders throughout the gulf region. Coast Guard, National Guard, and police helicopters helped ferry stranded victims from their rooftops. Paramedics treated the wounded and dehydrated. Department of Homeland Security officials attempted to coordinate relief efforts and maintain the flow of supplies. The emergency response lasted for weeks, with many responders still on the ground long after the waters had receded.

In the initial days of the response, there were significant problems with communication, especially between local and federal responders. According to the House subcommittee investigating the response to Katrina, a lack of interoperability meant that "first responders in helicopters could not talk to crews patrolling in boats, and National Guard Commanders in Louisiana and Mississippi had to use runners to relay orders"[1] (Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). This lack of communication led to a significant slowdown in rescue operations and has prompted many critics to question if interoperability could have saved some of the thousands of people who succumbed to flood waters along the gulf coast.

Two common themes bind the above incidents. First, they were all large-scale events that required a massive emergency response from a number of agencies. Federal, state, and local responders from a number of disciplines and jurisdictions were involved in each. Second, these responders were not able to communicate with each other via

[1] These compatibility problems were exacerbated by a lack of operability. In many cases the storm had knocked out the communication infrastructure that could have at least provided some communication between the various response agencies.

radios. This lack of interoperable communication substantially increased the danger to both emergency personnel and civilians, and in some cases led to devastating results.

Interoperability between emergency responder communication systems has been a recognized need in the public safety community for over 30 years. However, it was only in the post-9/11 era that the federal government became heavily involved in finding a solution[2]. Billions of dollars and hundreds of thousands of working hours have been put towards giving first responders the ability to talk outside their own agencies. But, despite numerous attempts to fix the problem from all levels of government, interoperability remains an elusive goal. In a 2006 survey by the National Governor's Association, 83% of state Homeland Security directors listed "Developing interoperable communications for first responders" as their number one priority (National Governors Association 2006). This shows that a lack of interoperability remains one of the most critical and pressing issues facing the emergency response community today.

Now, as the country nears the fifth anniversary of the September 11 attacks, two pertinent questions arise. First, has the federal government implemented good policies towards emergency responder interoperability, and second, is the United States sufficiently positioned to finally solve this problem in a reasonable amount of time? The answer to the first is generally yes – the federal government has made useful policy decisions that are helping to create interoperability in states and localities. But as for the second question, the outlook is not so clear. There are still many hurdles to overcome before interoperability is pervasive, and swift action must be taken to speed the process along.

---

[2] The United States military dealt with issues of interservice interoperability much earlier, but their efforts had little effect on challenges faced by the public safety community. For more information on the military efforts towards interoperability, see Chapter 5.

Interoperability: A Complex Problem

Interoperability is a simple concept with hundreds of complexities. The general definition of interoperability is responders from different agencies being able to talk to each other. However, inside that simple definition lurks a number of difficult questions. Does interoperability mean that every firefighter at the scene of an incident should be able to talk to every police officer? Or is it sufficient that the incident commanders from each agency can communicate? If a radio system takes one second to relay a message to different radio system, is it interoperable? What about five seconds? Twenty seconds? Does achieving interoperability require the transmission of data as well as voice? Does it include communication with federal response agencies as well as state and local officers? National Guard and military? State and local elected officials, such as a mayor or governor?

Just as important is the question of the level and consistency of interoperability. Oklahoma City, Columbine, September 11, and Hurricane Katrina were catastrophic and well-publicized examples of the need for interoperable communication. But there are numerous other small-scale examples of state and local emergency responders needing to communicate with each other and not being able to (National Task Force on Interoperability 2005). These occur especially near the edges of jurisdictions, or when incidents become too large to be handled by a single response agency. Is interoperability a necessary component of day-to-day emergency response, or is it only required in the event of major catastrophes?

Further complicating matters is the fact that every response agency has different interoperability problems and different ways of approaching them. There are over 60,000 emergency response agencies in the United States, at the local, state, tribal, and federal

level. These agencies, which own and operate over 90% of the nation's public safety wireless infrastructure, are largely autonomous and have the freedom to make their own decisions regarding what equipment to buy, what technology to use, and what policies to implement. The individual state and local response agencies also have the sole authority to decide which other agencies they want to partner with to establish interoperability. The federal government has some power to set interoperability guidelines, but at the end of the day it is up to the states and localities to determine their own level of interoperability (Boyd 2005).

Interoperability can mean a number of things to a number of people, but in order to facilitate a meaningful discussion, bounds must be placed on its definition. First, unless explicitly stated otherwise, "interoperability" in this paper refers to wireless communications interoperability. Specifically, this refers to the ability of emergency responders to share information via voice and data signals over radio waves. There are federal efforts underway to make other types of information exchange between response agencies compatible, such as the development of common credentials and badges to facilitate rapid responder identity verification (Torres Interview 2006). These efforts are sometimes also referred to as "interoperability," but they fall outside the focus of this thesis.

Second, interoperability, in its ideal form, encompasses a number of features. For a communication system to be considered truly interoperable it should:

- Allow communication with all other local emergency response agencies which have overlapping or adjacent jurisdictions;
- Allow communication with all emergency response agencies from higher levels of government, including the surrounding county, state, and federal agencies;

- Provide on-demand service without requiring the deployment of special equipment at the scene of an emergency;
- Provide real-time service that does not suffer from noticeable delays;
- Provide secure service that can adequately direct the flow of information; and,
- Provide a transparent end-user experience, which does not require significant time to access interoperable functionality.

Systems which only meet some of the above criteria are still valuable, but in this paper they will be referred to as "partially interoperable." Only systems that meet all six of the above criteria will be considered fully interoperable.

Additionally, the terms "emergency responders" and "first responders" will be used interchangeably to describe the various public law enforcement, firefighting, and medical teams that might respond in the first few hours of an emergency. There are some questions in both the literature and in the response community about whether a building's security officers are "first responders" or if HAZMAT teams, for example, should be termed "second responders," since they arrive after a response has already started (Doherty Interview 2006). While these distinctions may be academically interesting, they only serve to muddle an already confusing issue. For this paper, a first responder is any public safety official who contributes on the scene of an emergency.

The Reasons for a Lack of Interoperability

In today's technology-driven world, interoperability seems like it should be easy. After all, cellular telephones made by different companies and operating on different service provider networks are able to communicate without incident. Laptop computers with wireless adapters have no problem communicating with the WiFi router at home, in the office, or at the corner coffee shop. Commercial, private, and military aviators are

able to communicate with any nearby control tower or aircraft. Why, then, is it so difficult for a firefighter and paramedic from the same town to talk to one another?

The National Task Force on Interoperability[3] cites five general reasons for a lack of interoperability: incompatible and aging communications equipment, limited and fragmented funding, limited and fragmented planning and coordination, limited and fragmented radio spectrum, and limited equipment standards (National Task Force on Interoperability 2005). These five causes are widely accepted as the major hurdles that a response agency must overcome when trying to achieve interoperability with other response agencies[4]. However, because each locality inevitably faces unique interoperability problems, the importance of each hurdle varies from agency to agency. Each of these causes can impact an agency's ability to be interoperable.

The first cause, incompatible and aging communications equipment, is probably the most frequently cited reason that responders lack interoperability. Incompatibility can be caused by a number of things, but in this context it most often refers to the implementation of proprietary and incompatible communication protocols. For example, when Motorola engineers a radio system, they must implement a protocol that designates how signals are sent and received between handheld radios. Motorola can adopt any protocol it wants, and unless it uses open standards, this protocol will probably not interface with the protocols of a Motorola competitor, such as Alcatel[5]. Thus, different emergency response agencies with radio systems manufactured by two different

[3] The National Task Force on Interoperability, formed by the National Institute of Justice in 2001, was designed to help educate state and local elected officials on the challenges to and benefits of achieving interoperability. Although the NTFI is no longer active, their work is still updated and distributed by the NIJ. More information on the NTFI can be found at http://www.ojp.usdoj.gov/nij/topics/commtech/ntfi/

[4] The majority of federal documents refer to these five causes as the definitive reason that a lack of interoperability exists.

[5] This problem of conflicting and proprietary protocols can be found throughout the emergency radio manufacturing industry, and is not solely representative of Motorola and Alcatel.

companies will most likely not be able to talk to each other[6]. The age of many systems is also partly to blame. Many of the communication systems being used by responders were purchased over 30 years ago, when interoperability was not a recognized concern for the user community or vendors (Boyd 2005). A number of systems that are still in use today were simply never designed with interoperability in mind.

Upgrading or replacing systems is a possibility, but it would be very expensive. A 1998 study put the cost for full nation-wide replacement at $18.3 billion[7], which does not take into account the extra cost for training, installation and maintenance of new systems (Public Safety Wireless Network 1998). Although there is some federal funding available, the majority of this cost would fall on state and local organizations. Limited and fragmented funding from local, state, and federal sources impedes interoperability by making it difficult to fund projects and purchase new equipment.

Even with unlimited funding, interoperability is not achievable without a concrete planning and governance model. Agencies from neighboring and overlapping jurisdictions frequently fail to meet with each other to discuss planned equipment purchases. This may be due to a number of reasons, from a desire to remain autonomous and retain organizational hierarchies, to jurisdictional rivalries, to a simple lack of foresight (Mayer-Schönberger 2005). Without consistent planning and coordination, interoperability efforts will be inefficient at best and failures at worse.

---

[6] This problem is compounded by the fact that equipment manufacturers may be reluctant to abandon proprietary protocols. The use of incompatible protocols tends to lock emergency response agencies into purchasing equipment from a single firm, in order to maintain backwards compatibility with previously purchased components.

[7] This number comes from a 1998 report, which is considered out of date now, despite being the most recent estimate available. The value of $18.3 billion is used here to convey a general sense of the enormity of cost associated with replacing the radio communication infrastructure in this country.

The fourth reason that agencies lack interoperability is fragmented spectrum. As can be seen in Figure 1-1, emergency responder radios currently operate in ten isolated frequency bands on the electromagnetic spectrum. Because of the physical properties of radio waves, no antenna is able to transmit or receive in all ten bands. Thus, if two adjacent response agencies operate in different bands, their radios will most likely be unable to communicate with each other.

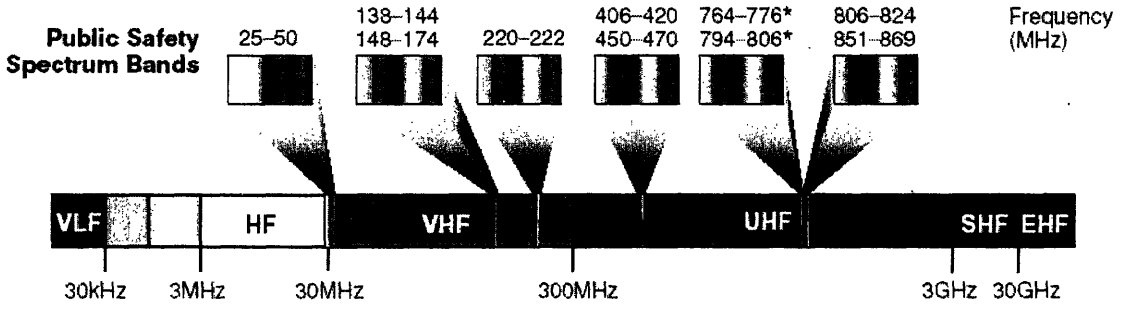

Figure 1-1 The 10 isolated bands of the public safety spectrum
Source: (Kentucky Wireless Interoperability Executive Committee 2004)

Finally, the fifth cause of interoperability woes – a lack of standards – relates closely to the incompatible equipment problem. Many of the currently deployed systems use proprietary standards because satisfactory open standards have not been widely available or supported until recently. The main open wireless emergency communication standard is known as Project 25 and it has been in development for 15 year. However, until late 2005, only one small part of that standard had been defined and its implementation across systems was inconsistent (Orr 2005). Some systems claiming to conform to the existing open standards still cannot interface with each other (Lipowicz 2005). Without widely supported and technically sufficient open standards, equipment manufacturers will have to rely on proprietary and incompatible communication protocols, which stymie interoperability.

When faced with these five main hurdles to interoperability, the temptation arises to immediately start looking for a silver-bullet solution. Unfortunately, no such solution exists. Having every emergency responder everywhere use the same radio system would conquer the technical problems of incompatible equipment and fragmented spectrum, but this solution is impractical for a number of reasons. It would be prohibitively expensive, require massive coordination by thousands of state and local agencies, not fit the needs of any one specific agency, and rob the state and local agencies of choice. Cellular telephones could be used to maintain communication between incident commanders from different agencies, but cell phones lack the ability to broadcast to multiple responders at once. Also, the telephone network can quickly become overloaded during an emergency and it lacks the robustness, reliability, and efficiency required for emergency operations (National Task Force on Interoperability 2005). Crosspatch and repeater technology can be helpful for bridging existing communication system, but no single piece of technology is right for every agency. Perhaps most important, no technological solution can be effective without coordination on the part of responders.

Any solution to the lack of interoperability must be multifaceted. It must incorporate a systems-of-systems approach that recognizes the need to blend existing and new technology. It must address all five of the causes of lack of interoperability and take into account the need for training, planning, and cooperation between different levels of government. Finally, it must be supported by the people who use it. If an interoperability solution does not meet the needs of first responders, it will be wasted.

The Federal Role: A Look Ahead

This chapter introduced the idea of interoperability and raised the question of federal involvement in solving the problem. The rest of this thesis will focus on the federal government's efforts to increase interoperability between emergency responders, and detail the work that still needs to be done.

Chapter 2 will focus on the technical aspects of interoperability. It will give a detailed overview of how emergency responder radio communication works, and discuss some of the short-term and long-term technologies that the federal government is advocating as potential solutions to interoperability issues.

Chapter 3 will detail the programs, policies, and organizational changes that the federal government has used to address the problems of interoperability. This chapter will carefully examine Project SAFECOM, the umbrella program for all federal interoperability efforts, which resides in the Department of Homeland Security.

Chapter 4 will provide analysis of these federal efforts, with a critical look at the progress that has been made across the nation. It will also provide some inspection of the federal money that has been put towards interoperability since September 11, and explore where the responsibility for solving the problem lies.

Chapter 5 will contrast the United States efforts against two very different cases of achieving interoperability – the public safety community in the European Union, and interservice interoperability within the U.S. military.

Finally, Chapter 6 will present recommendations for improving federal policies towards interoperability, and offer some solutions for further reducing the interoperability problems that emergency responders face.

References

Boyd, David. 2005. United States Senate Committee on Commerce, Science, and Transportation. *Testimony of David Boyd, Ph.D.* September 29, 2005.

Doherty, Vin. 2006. Personal Interview. Washington D.C., March 29, 2006.

Kean, Thomas, Lee Hamilton, and et al. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Company.

Kentucky Wireless Interoperability Executive Committee. 2004. *Commonwealth Takes Interoperability Training on the Road*, April 2 2004 [cited April 11 2006]. Available from http://archives.techlines.ky.gov/april2004/interop.htm.

Lipowicz, Alice. 2005. NIST, Safecom to validate first responder radios for interoperability. *Government Computer News*, 9/23/2005.

Manzi, Catherine, Michael Powers, and Kristina Zeterlund. 2002. Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study. In *Terrorism Study Series*: Chemical and Biological Arms Control Institute.

Mayer-Schönberger, Viktor. 2005. The politics of public safety communication interoperability regulation. *Telecommunications Policy* 29:831-842.

National Governors Association. 2006. 2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships. Washington, DC: NGA Center for Best Practices.

National Task Force on Interoperability. 2005. Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives. Washington, DC: National Institute of Justice.

Orr, Dereck. 2005. United States Senate Committee on Commerce, Science, and Transportation. *Testimony of Mr. Dereck Orr*. September 29, 2005.

Public Safety Wireless Network. 1998. LMR Replacement Cost Study Report. Washington DC: Public Safety Wireless Network.

Rosegrant, Susan, and Arnold Howitt. 2001. The Shootings at Columbine High School: The Law Enforcement Response. Cambridge, MA: Kennedy School of Government, Harvard University.

Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. 2006. A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. Washington, DC: U.S. House of Representatives.

Torres, Nelson. 2006. Personal Interview. Telephone, March 31, 2006.

Chapter 2 – Technology's Role in Interoperability

Technology is a critical component of the interoperability problem, and it is often the first one that is addressed by policymakers. All wireless public safety communication networks use some type of specialized technology, including transmitters, towers, repeaters and handheld radios. For any proposed interoperability solution, the technical details of an underlying system must be taken into account before that solution can be effectively deployed. While governance and policies play just as important a role in establishing interoperability, it is, at its core, a problem that is based on technology.

There are a number of proposed technical solutions that address some or all of the causes of noninteroperability. These include a radio that automatically tunes in to the frequencies of the radios around it, a vehicle-deployed cross-patch system that dynamically links two base stations together at the scene of an incident, and a retransmitter that takes audio from one radio system and broadcasts it out on another. Some manufacturers have even proposed using internet protocol (IP) as a common interface between existing radios (Grimes 2005). The distinction and details of the various solutions can quickly become overwhelming, especially when looking for cross-cutting and comprehensive technological solutions. Further complicating matters is the fact that the state of available technology is constantly in flux. Some of the needed devices are available now, but some will not be ready for deployment for many years to come. Some systems are simple and proven, while others are experimental and require frequent expert tweaking.

Unfortunately, engineers have not yet developed a silver-bullet technology that will solve the nation's interoperability woes. However, they have developed a number of products and engineering concepts that attempt to alleviate parts of the problems. This chapter will first explain the basic technology underlying emergency responder radios. It will then examine some of the solutions that do exist and will analyze their uses and effectiveness. Finally, it will look at long-term technical solutions that are currently in development, and evaluate these solutions against present needs.

Emergency Radios: A Primer

Before examining the possible technical solutions to the interoperability problem, it is important to understand how radios, and specifically emergency radios, currently work. All wireless radio communication occurs through the transmission of oscillating radio waves. Each radio wave is characterized by frequency and amplitude[8]. These frequencies all fall somewhere within the radiocommunication spectrum, which is a subset of the electromagnetic spectrum with wavelengths that range between 0-300 GHz.

Not all frequencies within the radiocommunication spectrum are created equal. Physical properties of different radio waves make some frequencies more useful for certain applications. For example, firefighter communication systems benefit from using lower frequencies because these frequencies are better able to penetrate buildings and are less susceptible to diffraction and distortion (Frazier, Hooper, and et al. 2003). The choice of frequency also determines how much data can be transmitted in a given amount of time. Generally, higher frequency transmissions indicate higher bandwidth and more information flow, because more data can be packed into each second of transmission.

[8] Frequency, or the number of cycles per second, is measured in Hertz. Amplitude, or the strength or power of a wave, is measured in Watts.

This is why FM radio, operating in the MHz range, transmits higher-fidelity music than AM radio, which operates in the kHz range (Manner 2003).

Radio waves are radiated through space by a transmitting antenna, and are then intercepted by antennas that are designed to receive signals within that range of frequencies. The type of antenna determines the radio's functionality. Some antennas, such as those found on FM radios, are able to tune into multiple frequencies. Other antennas, such as those found on walkie-talkies and cellular telephones, are able to both transmit and receive radio waves, although only some can do so simultaneously.

A given radio will operate on a specific frequency or within a range of frequencies. The frequency can be subdivided into a number of voice channels which can range in size from about 5 kHz to 50 kHz, depending on the type of radio and the bandwidth of the frequency. So even if a radio is only able to receive signals between 720 and 721 MHz, it could still easily be tuned to 200 separate channels in that range. Intuitively, as the frequency increases, the number of available channels increase, so comparatively low-frequency radios operating between 800 and 810 kHz would only be able to squeeze out two distinct voice channels.

There are two main types of first responder radio systems: conventional analog and digital trunk systems (National Institute of Justice 2002). Both of these types of systems can suffer from a lack of interoperability. Analog systems are much older and use more simplistic architectures[9]. Responders on analog systems tune their radios to the frequency channel they wish to talk on, and they can then communicate with other responders within their agency that are on that channel. In most municipalities, channels

[9] Conventional analog systems are generally used only in smaller cities, towns, and rural areas. The majority of large cities have upgraded to digital trunked systems.

are designated for specific uses. For example, one channel might be designated for communication with the dispatcher while another is designated for incident response or ad-hoc communication with responders in the immediate area. Some larger organizations, such as metropolitan police and fire departments, reserve additional channels for incident commanders, detectives, HAZMAT teams, forensic units, and other working groups (Doherty Interview 2006). By restricting communication to appropriate channels, emergency responders are able to communicate with who they need to, when they need to, within their own organizations.

Conventional analog radio systems have several limitations, especially when they are used by large organizations. Generally, with analog systems, a given channel cannot have more than one user transmitting at a time. If two responders simultaneously attempted to contact a dispatch center, one would have to wait until the other was finished. While this problem is not serious in cases of two or three simultaneous transmissions, it grows considerably when an incident has hundreds of responders on scene. Compounding the problem is the fact that most conventional radios only operate in a half-duplex mode – they cannot receive communication when they are transmitting. Compared to a full-duplex device, such as a telephone or digital radio, half-duplex radios can result in missed communications and inefficiency.

Digital trunked systems are the other major type of radio used by first responders. These devices were first introduced in the late 1980s and have experienced increased popularity as cities upgrade their communication systems. Instead of designating specific channels within a frequency band for specific uses, trunked radios use a central computer to assign users to a "talk group". The computer then dynamically and transparently

assigns an open channel from the "trunk" of available channels whenever a user needs to communicate with his or her talk group. It then rebroadcasts that transmission on the channels of the other users in the talk group. Thus, communications between the same set of individuals might be seamlessly occurring over several different physical channels. The user does not have to fiddle with frequencies or wait for the channel to clear before transmitting – the computer handles it all.

Unfortunately, with the increased efficiency comes the increased complexity of the system. Digital trunked systems require more infrastructure and maintenance, which leads to higher cost. They also require a separate channel for system messages that coordinate which users are communicating with each other. In areas where the available channels are limited, it might be difficult to justify the sparing of an entire channel for control signals. Finally, digital trunked systems have traditionally used proprietary protocols for synchronizing and transmitting communications. Thus, digital trunked systems tend to require that all users are using equipment from the same manufacturer, which presents additional barriers to interoperability[10].

Non-Technical Workarounds to Interoperability

In Chapter 1, there was a somewhat trivial solution to the interoperability problem. If every emergency responder in the country uses the same radio system and operates in the same frequency range, then they will all be able to talk to each other. While this solution is impractical, both due to the cost of replacement and the coordination that it would require, there are other non-technical workarounds that provide some degree of interoperability at a minimum of cost. These workaround solutions are

[10] For more on the interoperability problems posed by proprietary protocols, see Chapter 3.

not as robust as those gained by introducing new technology, but they can serve as temporary fixes for those jurisdictions that are unable to upgrade.

One easy solution is for response agencies in the same geographic area to trade radios. Fire departments and police department could have extra radios that could be handed out to members of the other agency during an incident. This would give at least some of the responders (perhaps team leaders) the ability to communicate between agencies. There are several downsides to this approach. Most notably, the radios would take time to distribute, which could impact the efficiency of a response. The responders would also have to carry an extra piece of bulky equipment and would not be able to have communications on a joint channel or talking group.

Response agencies could also designate an "interoperability channel" throughout a geographic region. For example, all responders in the state of Massachusetts would know that Channel 24 in the 764 MHz frequency should be used for messages between agencies. This approach can be simple to implement, but it requires that all radios operate in the same frequency band, and have the same communication protocols. This approach also inevitably leads to a very congested interoperability channel during a major event, and prevents the benefits of different working groups operating on different channels.

Finally, while forcing a single nationwide communication system on all response agencies is financially and logistically impractical, agencies in small or isolated municipalities could implement this strategy on a smaller scale. In many cases, it is logical for the fire department and the police department of the same town to agree on a common system before overhauling their radio infrastructure. They could then have seamless interoperability with each other in most day-to-day occurrences that require a

joint response. However, if a larger event occurred that required the aid of state and federal agencies or neighboring cities, the interoperability problem would return. Also, a single system might not meet the operational needs of two different types of agencies, because agencies can use radios in very different ways (Doherty Interview 2006). There would need to be strong coordination and planning between the affected agencies, especially in determining how to divide and manage the cost of the shared system.

Short-term Technical Solutions

The non-technical workarounds can be inexpensive and simple to implement, but they do not provide the level of interoperability or reliability that many emergency responses require (National Task Force on Interoperability 2005). Solutions involving technology can offer more options, especially for those public safety agencies that need seamless and transparent interoperability. There are currently three types of short-term technical solutions and a number of vendors that provide devices in each type (National Law Enforcement and Corrections Technology Center 2003).

The first technological solution is multiband radios. Multiband radios have two or more receiver/transmitter assemblies in a single walkie-talkie. These allow responders to tune into multiple frequencies at the same time, even if the frequencies are in different frequency bands. This is especially helpful to overcome the problem of fragmented spectrum. It is important to note, however, that these devices do not repeat signals from one network to another, so only those responders with multiband radios will be considered interoperable. The systems themselves are not linked, so responders with single-band radios will still be unable to communicate outside their agency. These devices also require that responders correctly program the radios to the frequencies of the

other responding agencies. While a police officer with a multiband radio will most likely preprogram the local fire department's frequencies, the introduction of a new agency – FEMA, for example – will require additional work on the part of the responder. Finally, because all of the interoperability components are integrated into the responder's handheld walkie-talkies, it is difficult to make multiband radios fit the small weight and size demands requirements by the users (Bischoff 2005).

Multiband radios are a good solution for linking individuals to multiple systems, but they require buying new radios for most responders in at least one local agency. To minimize the infrastructure upgrades and the changes to existing systems, response agencies should consider the use of system-to-system gateways that rebroadcast the transmissions of one system over another. These devices, also called crossband devices because they usually rebroadcast into another frequency band, can range in complexity from simple mobile repeaters to complex communication systems. The two major classes of crossband devices are console patches and audio baseband switches.

Console patches are circuits that patch together two or more audio signals at a communication or dispatch center. They provide the physical connections between two or more audio devices, and can be used to patch radios to radios or radios to telephone systems. Although older systems required operators to physically link the console patch to the transmission hardware, current console patches rely on computers to establish virtual links (NLECTC 2003). It is important to note that console patches generally require hardware from all involved agencies to be physically installed at the same communication or dispatch center, or linked by fiber optics. Console patches are beneficial because they can link both audio and data or control signal transmissions.

However, they require a significant amount of setup, and new agencies that come onto the scene of an incident cannot be rapidly added to the architecture.

Audio baseband switches overcome those difficulties because they do not physically connect the hardware of two communication systems like console patches do. Instead, baseband switches rebroadcast audio signals from one communication system to another. Generally, one radio from each agency is connected to the switch. These radios are then used for receiving and rebroadcasting transmissions that come across the various systems. This does require that each agency reserve one channel for interoperable messages, but these channels do not have to be in any specific frequency band (NLECTC 2003). Additionally, audio switches can be deployed in either fixed or mobile locations. In the event of a major incident, a truck containing the switch will be deployed along with responders and the system can be almost immediately configured to link all the responding agencies. These devices do suffer from the fact that they do not pass on any control information, so messages passed through a trunked system, which dynamically assigns channels, may not transmit correctly.

Long-Term Technical Solutions

Multi-band radios, console patches, and audio baseband switches provide immediate partial solutions to the interoperability problem. However, each has drawbacks which make them only suitable as stopgap measures. In order to truly eliminate a lack of interoperability, future systems must be able to overcome the problems posed by incompatible protocols, limited spectrum, and outdated technology. Two long term technical solutions are attempting to do just that.

The first long term technical solution to interoperability is the implementation of standards-based shared systems (Boyd Interview 2006). These systems would be digital trunk systems that employ standardized protocols to regulate who is talking on which talking group. By conforming to well-defined public standards, equipment manufacturers can ensure that their radios are compatible with radios developed by other firms. By combining this technology with the next generation of multiband antennas, manufacturers can also ensure that their antennas will operate in the biggest range of spectrum possible. In this way, two public safety agencies with two different radio systems will be able to immediately communicate, without patching their infrastructure together, rebroadcasting their signals, or otherwise jury-rigging their technology. Standards are currently being developed and finalized, and products with full standards support will be available by the end of the decade (Orr Interview 2006).

The second long term technology is known as software defined radio (SDR). Software defined radio is different from traditional radio, because the device's functionality and signal processing is handled by embedded software. Theoretically, this permits an SDR device with the right software to function as any radio device imaginable, from an emergency responder radio to a cellular telephone to a garage door opener (National Task Force on Interoperability 2005). It also permits the radio to receive and transmit signals on any frequency or with any protocol, eliminating the two major technical impediments to interoperability. Although several manufacturers are currently offering some SDR products, the technology is still several years away from widespread use in the emergency responder community (Boyd Interview 2006).

Summary and a Look Ahead

Technology has an important role to play in establishing interoperability. There are numerous non-technical and technical solutions that can provide varying levels of interoperability for emergency responders. Table 2-1 contains a breakdown of the solutions that were examined in this chapter and identifies the pros and cons of each. While neither the solutions listed nor the dimension by which they are measured should be considered an exhaustive list, this table gives a flavor of the types of choices that public safety agencies must make when evaluating new technology.

	Inexpensive	Quick on-scene setup	Easily interoperable with new agencies	All responders at scene are interoperable	Agencies can keep existing spectrum	Responders can use multiple channels	Responders can use multiple vendors
Swap radios	●	◍	◍	○	●	○	●
Designated cross-agency channel	●	●	◍	●	◍	○	◍
Single shared system	○	●	○	●	◍	●	○
Multiband radios	◍	◍	◍	◍	●	○	◍
Console patch	◍	○	○	●	●	●	◍
Audio baseband switch	◍	◍	●	●	●	○	●
Standards-based systems*	○	●	●	●	◍	●	●
Software radio*	○	●	●	●	●	●	●

Performance:
● - Good
◍ - Adequate
○ - Poor

Table 2-1 Performance of various interoperability solutions
*** = Limited current availability**

While technology is critical for interoperability, policy set at all levels of government is just as important. The next chapter will examine the policy decisions that were made by the federal government to promote interoperability in a post-9/11 world.

References

Bischoff, Glenn. 2005. DOJ seeks ideas on public-safety radios. *Mobile Radio Technology Magazine*, December 1, 2005.

Boyd, David. 2006. Personal Interview. Telephone, March 27, 2006.

Doherty, Vin. 2006. Personal Interview. Washington D.C., March 29, 2006.

Frazier, Patricia, Robert Hooper, and et al. 2003. Current Status, Knowledge Gaps, and Research Needs Pertaining to Firefighter Radio Communication Systems. Arlington: TriData Corporation.

Grimes, Brady. 2005. *Cisco debuts integrated IP-based radio system*. Government Computer News, October 24 2005 [cited March 4 2006]. Available from http://www.gcn.com/online/vol1_no1/37399-1.html.

Manner, Jennifer. 2003. *Spectrum Wars: The Policy and Technology Debate*. Norwood, MA: Artech House.

National Institute of Justice. 2002. Guide for the Selection of Communication Equipment for Emergency First Responders.

National Law Enforcement and Corrections Technology Center. 2003. Guide to Radio Communications Interoperability Strategies and Products. Rome, NY: AGILE Program.

National Task Force on Interoperability. 2005. Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives. Washington, DC: National Institute of Justice.

Orr, Dereck. 2006. Personal Interview. Washington DC, March 29, 2006.

Chapter 3 – Federal Policy towards Interoperability

Interoperability is a problem that occurs at the state and local levels of government. It is the state and local public safety agencies that suffer when their emergency responders cannot communicate, and it is these same agencies that are ultimately responsible for solving the problem. However, on September 11, 2001, the nation realized that interoperability was too important a problem to be left to states and localities alone. Emergency responders were suddenly faced with a new and imminent threat of international terrorism, and many of them were ill-prepared to face the technological and operational challenges that such a threat imposed (Rudman, Clarke, and Metzl 2003). Given the likely possibility of future terrorist attacks and the probability that these attacks would be high consequence events requiring the collaboration of multiple agencies from multiple jurisdictions and disciplines, the lack of responder interoperability suddenly became a national security issue. Thus, September 11 prompted the federal government to make a number of organizational and policy changes to improve the national level of interoperability.

Prior to September 11, there had been few federal non-military programs that examined and promoted interoperability. The ones that did exist were limited in scope and effectiveness. Federal advisory committees, like the Public Safety Wireless Networking (PSWN) working group, had analyzed the problem and made recommendations, but the onus was on the response community to adopt these recommendations. The federal government had provided little in the way of incentives or consequences for compliance with these recommendations, and they had few programs in

place to assist emergency responders in purchasing new interoperability equipment. Today, the federal interoperability landscape looks much different.

Chapter 1 highlighted five causes of noninteroperability: incompatible and aging communications equipment, limited and fragmented funding, limited and fragmented planning and coordination, limited and fragmented radio spectrum, and limited equipment standards. The first three of these causes can be addressed by federal policies that have immediate impact on the nation's level of interoperability. The last two, spectrum and standards, will have a more long-term impact. This chapter will detail the numerous federal efforts that have addressed or are addressing interoperability in the post-9/11 world, both from the legislative and executive branches of government. It will first look at how these efforts have been divided organizationally and will then focus on programs and policies that are designed to mitigate the five causes of noninteroperability.

Organizational Makeup of Federal Interoperability Programs

Organizational charts rarely tell the whole story, but they can be useful places to start to examine how an organization approaches a problem. In the federal government, no single department or agency is wholly in charge of all federal interoperability programs. The Department of Homeland Security (DHS), created, in part, to provide federal resources to state and local responders, is an obvious choice for a lead agency. In fact, SAFECOM, a program within the DHS Office of Interoperability and Compatibility, defines itself as "the umbrella program within the federal government to coordinate the efforts of local, tribal, state and federal public safety agencies working to improve... interoperable wireless communication" (Jenkins 2003). However, interoperability programs also exist in the Department of Justice (DOJ), the Department of Commerce

(DOC), the Federal Communications Commission (FCC), and even other areas of DHS (see Table 3-1 for a list of major programs). While SAFECOM coordinates with these programs and agencies, it does not control their budgets or directly authorize their activities. Thus, there is no single nexus point for all federal interoperability policies or decisions.

Program Name	Department	Mission and Activities
SAFECOM	DHS	Oversees all initiatives and projects pertaining to public safety communications and interoperability
Office of Grants and Training	DHS	Provides funds to state and local emergency response community for the purchase of new equipment
Integrated Wireless Network	DOJ	Provide a consolidated nationwide wireless communications service for federal law enforcement and its agents
CommTech	DOJ	Assist state and local law enforcement by developing, testing, and evaluating interoperability solutions and products
Community Oriented Policing Service (COPS) Interoperable Communication Technology Program	DOJ	Provides grants to law enforcement for researching or purchasing new interoperable communications equipment
NIST Public Safety Communications Systems	DOC	Develop standards for public safety wireless communication
Wireless Telecommunications Board: Public Safety	FCC	Manage spectrum allocation for public safety communication, including new spectrum being appropriated for interoperability

Table 3-1 Major Federal Programs that Impact Public Safety Interoperability
Sources: (Victory et al. 2005) and (Orr Interview 2006)

Although there are many programs now, there were even more in the first years after September 11. Two additional programs – the aforementioned Public Safety Wireless Network (PSWN), a joint effort between the DOJ and the Treasury Department, and the Advanced Generation for the Interoperability for Law Enforcement (AGILE)

program, which was under the DOJ – were shut down in 2003 and 2005 respectively[11]. These programs were thought to partially duplicate the efforts of other government programs, especially SAFECOM[12] (Chandler 2003), and were deemed superfluous. The fact that they were shut down indicates that the federal government is working to streamline the organizational components that address interoperability problems.

SAFECOM's own complex organizational history bears mentioning. The program was originally conceived of several months prior to the 9/11 attacks as one of President Bush's possible "e-government" initiatives. In October 2001, only a few weeks after those attacks, SAFECOM was stood up in the Department of the Treasury. Management problems and a lack of clear mission alignment with the Treasury prompted the administration to move SAFECOM into FEMA[13] in March 2002 (Koontz 2004). Under FEMA leadership, SAFECOM went through two management teams before being transferred to the DHS Science and Technology Directorate when the Department was stood up in 2003. Although it still remains in the S&T Directorate, a new parent office was created for it in 2004. This new Office of Interoperability and Compatibility was designed to give the program more visibility within the public safety community, while allowing it to retain its original mission objectives (Boyd Interview 2006).

Having more than a half dozen offices and programs working on the same general problem requires significant coordination and oversight to prevent duplicative efforts. Since 2003, when it was placed within the S&T Directorate, SAFECOM has adopted the organizational responsibility to build partnerships and shared policies with those

[11] Both the PSWN and AGILE were operating before September 11.
[12] Documents produced under both AGILE and PSWN remain available in SAFECOM's online library which can be found at: http://www.safecomprogram.gov/SAFECOM/library/
[13] At this time, FEMA was still an independent agency. It would not become a part of DHS until DHS was created in March 2003.

interoperability-focused agencies that exist elsewhere in the federal government (Boyd Interview 2006). This effort has not been undertaken easily. A 2004 GAO report found that SAFECOM initially had trouble establishing agreements and Memorandums of Understanding with its federal partners (Koontz 2004), but continued collaborations and compromises have overcome most of those interagency roadblocks (Boyd Interview 2006). Although SAFECOM does not have direct control over the budgets and activities of the law enforcement-focused components of DOJ or the spectrum-focused components of the FCC, those agencies, as well as the other federal interoperability agencies, now take direction from SAFECOM's interoperability policy initiatives.

Funding and Facilitating New Equipment Purchases

One of the key roles of the federal government is to help state and local emergency response agencies purchase the right equipment as it becomes available. As seen in Chapter 2, there are a number of technical solutions that provide varying levels of interoperability that are either available now or will be available soon. While a majority of the money for buying new equipment is generated at the state and local level – through taxes, bond issues, and state grants – the federal government has an important role to play, both in issuing money for interoperable communications and helping public safety agencies make good choices about which technology they ultimately purchase.

Ever since September 11, the federal government has realized that first responder interoperability is a national security problem, and not just a state and local problem. To help foster interoperability, the federal government has reportedly issued over $2 billion towards communication systems since 2001[14] (Office of Management and Budget 2006).

[14] The $2 billion estimate is somewhat questionable and is given closer inspection in Chapter 4.

Federal money to upgrade state and local communication systems is issued from both the Department of Homeland Security and the Department of Justice, usually in the form of grants. Within DHS, the Office of Grants and Training is in charge of evaluating grant requests and distributing funds. Within DOJ, the Community Oriented Policing Service (COPS) fulfills that role. In both cases, SAFECOM is in charge of developing the grant guidance and application criteria that ensures federal money is being used to foster interoperability (Boyd Interview 2006).

Federal interoperability grants help states and localities patch existing networks together, and they help fund the replacement of complete communication systems (Levy 2006). Regardless of size and use, all interoperability-focused grants require that the state or local applicant address a number of issues in their proposal. First, they must describe how the equipment they buy will improve technical interoperability with those agencies around them. They must also define the governance structure and Memorandums of Understanding that exist between their agency and the surrounding agencies. If the applicant is a state entity that will then redistribute funds to localities, the state must identify the local input they received in formulating the grant, to ensure that the people who will actually be using the technology have had sufficient input into the process (Project SAFECOM 2005b). These various requirements are designed to ensure that all federal emergency responder communication grants are put towards their best use possible, and contribute in some way to increasing interoperability (Boyd Interview 2006).

Besides individually distributed block grants, there have been several other initiatives that the federal government has used to improve interoperability around the

nation. One of the most important was RapidCom 9/30, a program that created a minimum level of incident-level interoperability for ten urban at-risk areas[15] in 2004. According to the DHS press release that was issued at the program's announcement, RapidCom was designed to "ensure that incident commanders have the ability to adequately communicate with each other and their respective commanders" within "an incident area approximately the size of the attacks on the World Trade Center towers" (Department of Homeland Security 2004). Recognizing that full and always-on interoperability was still a long-term priority, RapidCom focused only on providing the selected cities with a minimum level of interoperability, generally by funding the purchase of console patches and crossband repeaters. It also provided assistance with setup, training, and maintenance of this new communication equipment. RapidCom was successfully completed in September 2004, with all of the targeted cities reporting a significant increase in interoperability (Boyd 2005a). The RapidCom initiative also resulted in a "lessons learned" document that helps public safety officials in other major cities evaluate and implement their own interoperability plans.

Besides providing funding, the federal government also evaluates the technology that is available and makes recommendations about what technology should be purchased. The number of "interoperability solutions" from multiple vendors can be enormous and overwhelming. Emergency responders are busy carrying out their day-to-day missions and often do not have the resources or expertise to evaluate multiple technologies (Boyd 2005b). Without federal guidance, first responders must either rely on manufacturer assurances or previous buyer reports to evaluate which technology to

[15] The urban areas were: New York, NY; Chicago, IL; Washington, DC and adjacent regions; Los Angeles, CA; San Francisco, CA; Philadelphia, PA; Houston, TX; Jersey City, NJ; Miami, FL; and Boston, MA.

buy. Unfortunately, these sources of information may lack the level of objectivity that is needed by many public safety agencies. The federal government can serve as the impartial data source that provides consistent and up-to-date evaluations of new technology and services.

Evaluations are meaningless without a common baseline to compare different systems. One of SAFECOM's first tasks was to establish formalized requirements that manufacturers are expected to meet. The resulting document, the Public Safety Statement of Requirements[16] (SoR), is intended to "[help] the public safety community convey a shared and vetted vision that ultimately will help industry better align research and development efforts with critical interoperable needs" (Project SAFECOM 2006). This document is a statement of functional needs, such as compatibility, usability and ergonomic requirements. Because it shies away from technical requirements, it gives manufacturers some liberty in how they fulfill the SoR. However, in many places, the document is very far reaching with its demands; some of the specifications involve handset biometric identification and real time foreign language translation, both technologies which are still years from commercial deployment. Altogether, this document provides a comprehensive, if somewhat long-term, expectation of the end user experience.

In order to evaluate the SoR requirements, as well as compliance with interoperability standards, NIST and SAFECOM have partnered to create a comprehensive testing and evaluation program (Lipowicz 2005). This Conformity Assessment Program, which is currently under development and scheduled for

[16] The Public Safety Statement of Requirements v1.1 can be found online at: http://www.safecomprogram.gov/SAFECOM/library/technology/1253_statementof.htm

implementation by the end of 2006, will produce "a sort of 'Consumer Reports' of [emergency responder communication] equipment" (Department of Homeland Security 2005). Once it is published, public safety agencies can then turn to that report and determine what features and level of compliance a given device or system has. Since this testing and evaluation program is still being developed, some details, such as how often and under what conditions systems will be evaluated, is not yet publicly known. Regardless of the final details, many public safety agencies are eagerly awaiting the Conformity Assessment Program's deployment (Doherty Interview 2006).

Other programs within the federal government also provide testing and evaluation of interoperable communication systems. Most notable is the National Institute of Justice's CommTech program within the DOJ. This program has already conducted one technical evaluation on a piece of interoperability equipment, the ACU-1000 console patch. This test used a combination of Federal laboratory assessments and operational test bed exercises for field evaluations (AGILE 2001). However, this evaluation occurred in 2001, and it is unclear what progress has been made on the other five systems currently listed as being evaluated (CommTech 2006). It is also unclear what collaboration, if any, the CommTech evaluation process will have with the SAFECOM/NIST Conformity Assessment Program.

Encouraging Collaboration

Providing new technology is obviously an important part of creating interoperability. However, according to many interoperability experts, the most important thing that the government can do is encourage collaboration between agencies. Dr. David Boyd, the director of SAFECOM, testified that "Technology is at the center of

[interoperability]..., but [it requires] serious agreements, planning, [and] governance kinds of arrangements across jurisdictions" (Stevens 2005). Dereck Orr, the Program Manager for NIST's public safety communication program, said that the most important thing the government can do is foster "Memorandums of Understanding, training and joint exercises" (Orr Interview 2006). Captain Vin Doherty of the FDNY joked that the best interoperability technology that DHS could develop is an "egonator pill" that would eliminate the egos of the various federal, state, and local agency leaders and bring them all to the same table (Doherty Interview 2006). In short, many experts agree that interoperability is impossible without collaboration at the state and local level.

The federal government recognizes the importance of coordination on an organizational scale as well. One of the first public documents ever produced by SAFECOM was the Interoperability Continuum, seen in Figure 3-1. This chart lists five different dimensions of interoperability: Governance, Standard Operating Procedures, Technology, Training & Exercises, and Usage. Of these five dimensions, four deal with how responders work together and assist each other to achieve interoperability. Only one, Technology, deals with the devices that responders use to communicate.

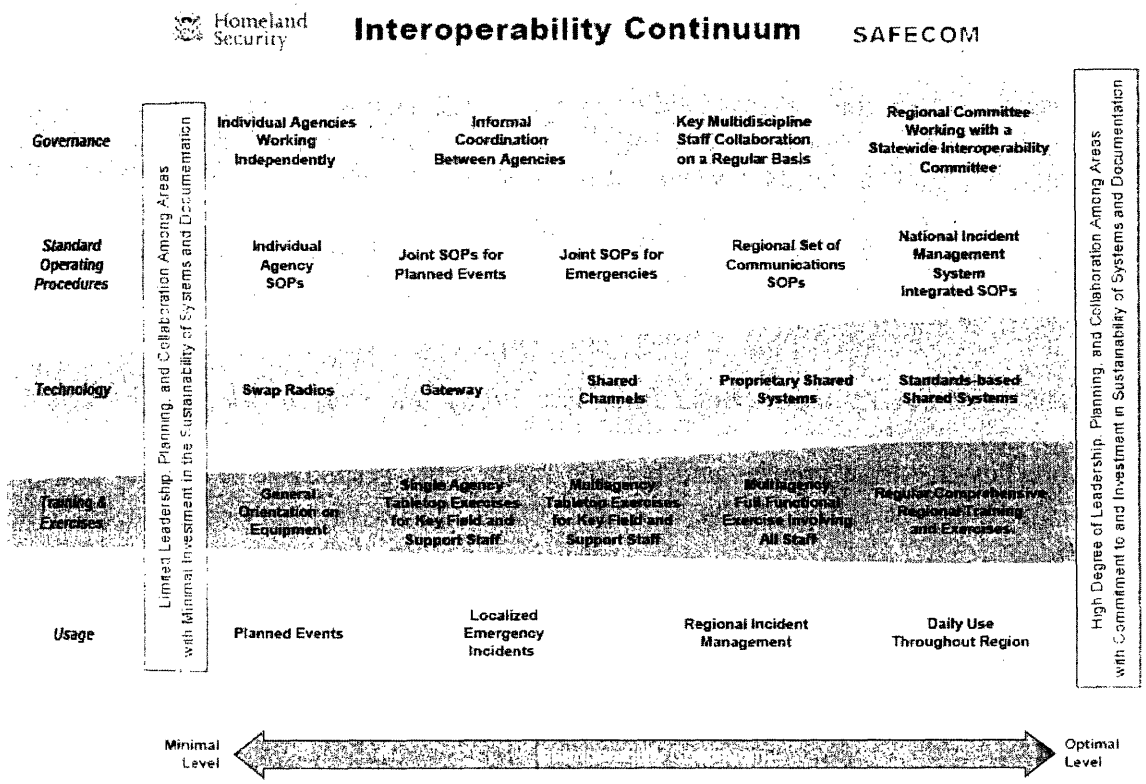

Figure 3-1 The Interoperability Continuum
Source: (Project SAFECOM 2005a)

Collaboration is critical to interoperability, but fostering it is a much more difficult problem than providing new technology. With 60,000 state and local public safety agencies, each with their own requirements and interoperability needs, there are almost a limitless number of relationships and governance structures that will exist between them. There is no easy template for achieving collaboration between agencies. Legal statutes, preexisting agreements, agency rivalries and personality conflicts can all also negatively impact the ability for a region to become interoperable. The federal government must tread lightly as it encourages coordination, so that none of the involved parties feel marginalized or withdraw from the process.

This last point is shown in the history of SAFECOM. In its first year of operation, SAFECOM was "seen as a top-down entity with a federal focus" and was unable to

garner widespread support for its activities (Gurss 2006). First responders were put off by its authoritarian style and did not believe that the federal government was in a good position to assess their needs. When SAFECOM was moved to DHS in 2003, it restructured itself to take a bottom-up approach. Instead of imposing recommendations from on high, it began to base almost all of its decisions on emergency responder and public safety community input (Boyd Interview 2006). As a result, the user base had much more buy-in to the process and became much more responsive to federal policy decisions.

In the last two years, Congress and the Department of Homeland Security have taken additional steps to foster collaboration between public safety agencies. In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress directed the Secretary of Homeland Security to quickly develop two regional pilot programs that would "develop a regional strategic plan to foster interagency communication... and coordinate the gathering of all Federal, State, and local first responders in that area" (*Intelligence Reform and Terrorism Prevention Act* 2004). These Regional Communication Interoperability Pilots, implemented in Kentucky and Nevada, brought members of the public safety community together in each state, so that they could come up with collaborative solutions to interoperability. Although the pilot programs are still ongoing, proponents report that they have been instrumental in "[helping SAFECOM] identify models for improving communications and interoperability" as well as providing a near-term increase in the interoperability of those two states (Boyd 2005b).

Freeing Spectrum

As discussed in previous chapters, public safety agencies suffer from fragmented and limited spectrum. In the United States, the FCC has licensed 10 different frequency bands of the electromagnetic spectrum for emergency responder use, ranging from 25 MHz to 870 MHz[17]. The physical nature of radio waves and antenna design prevents a single radio from being able to reach more than two or three of these different bands. For efficiency and to prevent interference, response agency communication equipment is usually designed to operate within only one or two of these bands. Thus, if two different public safety agencies have communication systems that operate in two widely separated bands, they will not be interoperable.

A lack of available spectrum also exacerbates the problem. Many of the technical fixes described in Chapter 2 require the use of extra frequency for passing interagency messages or control data. With public safety agencies confined to narrow chunks of scarce spectrum, they are unable to implement some of these solutions (National Task Force on Interoperability 2005). Although these spectrum issues are generally confined to major cities, they still pose significant challenges for emergency responders. As the director of SAFECOM phrased it, "[spectrum scarcity] only affects 15% of the country, but it impacts 85% of the population" (Boyd Interview 2006).

Spectrum is a finite and valuable resource, one that has been highly regulated in this country since the early days of radio. For many years now, all spectrum that is

[17] This fragmented approach occurred partially by accident and partially by design. In the 1950s and 1960s, as cities grew and more first responders began to use radio systems, the need for public safety spectrum increased. The FCC allocated patches of available frequency as existing spectrum became overcrowded, but often had to choose non-adjacent patches because all nearby frequencies in the spectrum had already been allocated to other purposes (National Task Force on Interoperability 2005). Some patches of frequency, however, were chosen for their physical properties. Low frequency transmissions are useful in rural areas, because they travel farther without distortion. High frequency transmissions are useful for transmitting large amounts of data, because the radio wave oscillates quickly.

technically suitable for radiocommunication has been allocated for some purpose (Manner 2003). In order to expand the amount of spectrum allocated to first responder radio communications, the FCC must take spectrum away from someone else. This presents both technical and political problems, because owners of spectrum have already made significant investment in infrastructure that is designed to operate on those frequencies. No one wants to lose spectrum that they have previously been granted.

In 1995, the FCC and the National Telecommunications and Information Administration[18] (NTIA) began to examine how the spectrum needs of the public safety community would change over the next 15 years. Together they established the Public Safety Wireless Advisory Committee (PSWAC), a group made up of public safety representatives, to determine how much additional spectrum responders would need by 2010. The PSWAC estimated that the public safety community would require an additional 97.5 MHz of radio spectrum to keep up with current growth, an amount much larger than the FCC had hoped (Public Safety Wireless Advisory Committee 1996).

To date, only 24 MHz of additional spectrum has been identified by the FCC as a good candidate for reallocation to public safety agencies. This spectrum, from 764-776 MHz and 794-806 MHz, was chosen for two reasons. First, it is close enough to the already allocated 36 MHz of public safety spectrum in the 800 MHz range to facilitate interoperability with devices on those frequencies. Second, it is spectrum that was previously allocated to infrequently used broadcast television stations[19].

---

[18] The National Telecommunications and Information Administration is in charge of regulating spectrum for federal agencies, as opposed to the FCC which regulates spectrum for state, local, and commercial entities.

[19] This spectrum in question comprises television channels 63, 64, 68, and 69 as well as some overlap into adjacent channels.

In 1997, Congress authorized the reassignment of this 24 MHz of spectrum in the 700 MHz band to public safety, on the belief that the television broadcast stations using that spectrum would begin to switch over to digital broadcasting. However, the television broadcasters have been slow to give up the use of their analog frequencies. In many major metropolitan areas, this spectrum that was allocated for public safety use is still being blocked by broadcast television channels, almost 10 years after the change was made in legislation (National Task Force on Interoperability 2005).

Although broadcasters were essentially squatting on spectrum that was no longer theirs, there was little that responders or the FCC could do. In the 1997 legislation, Congress had said that broadcasters were not required to give up that spectrum until December 31, 2006 or until 85% of the broadcast market had the equipment to receive digital signals, whichever was later. Since digital equipment penetration has been low, there was no certain date when the spectrum would be available. Radio manufacturers and emergency responders were reluctant to invest in developing or purchasing equipment that used this new spectrum, because there was no guarantee that it would ever be viable (Boyd Interview 2006). However, following Hurricane Katrina, and lobbying from the responder community and government agencies such as SAFECOM, Congress reevaluated its position on the spectrum issue. In legislation in early 2006, Congress mandated that broadcasters must vacate the channels by February 17, 2009 (Deficit Reduction Act 2005). It is expected that, once it is finally usable, this additionally allocated spectrum will go a long way in eliminating interoperability problems for those public safety agencies that are in large metropolises with overcrowded radio waves.

Creation and Implementation of Standards

As discussed in previous chapters, a lack of open and non-proprietary standards is one of the critical impediments to interoperability. If systems from one vendor transmit signals that cannot be understood by a system from another vendor, then it is impossible for agencies using those two systems to communicate. Dereck Orr testified that, "in the absence of standards, achieving... interoperability would be impossible" (Orr 2005).

The emergency response community recognized the need for open standards years ago. In 1989, a group of officials from the local, state, and federal public safety associations and agencies met together to determine the best way to define standards that would both ensure radios from different vendors would be interoperable and would create a more competitive marketplace for communication systems (Project 25 Steering Committee 2006). The result was Project 25 (P25), a set of standards that would be developed by a steering committee of public safety officials with technical support from the Telecommunications Industry Association (TIA).

The TIA and the P25 Steering Committee conceived of P25 as a suite of standards that would define eight of the interfaces necessary in a digital land mobile radio system. These include mobile-mobile communication, mobile-base station communication, console-console communication, and several others[20]. These standards, once properly defined, could be implemented by equipment manufacturers and the public safety community would then be able to purchase "P25 Compliant" devices that would communicate with other P25 devices, regardless of the manufacturer.

[20] For a complete list and technical description of the eight interface standards specified by Project 25, please see http://www.p25.com/resources/P25TrainingGuide.pdf

Unfortunately, the progress of Project 25 was very slow. Until late 2005, over 15 years after Project 25 was first initiated, only one of the P25 interfaces had been advanced to a level where it could provide an acceptable level of interoperability. This interface, the Common Air Interface, defines the wireless access between multiple handheld units or between handheld units and base stations. While this is a critical step towards achieving interoperability, according to Mr. Orr, the Common Air Interface alone is not enough. "The remainder of the interfaces either remains undefined or lacks enough specificity to allow for a common implementation of the interface...resulting in systems that do not meet the 'interoperability' requirements defined by the steering committee" (Orr 2005). In other words, before 2005, manufacturers could produce systems that conformed to the unfinished P25 standards but would still not be able to talk to each other.

There are several contributing reasons for the slow development of these standards, but the most important one resulted from a tussle between the various stakeholders involved in the P25 development process. The public safety representatives that made up the P25 Steering Committee were generally enthusiastic about getting all eight interfaces formalized quickly, because of the positive impact it would have on emergency operations. However, they had very specific performance requirements that the standards needed to address. On the other end of the scale were the equipment vendors and manufacturers, who were reluctant to change their already developed protocols to fit new open standards. A shift to open standards would require that they reengineer components of their entire product line, and it would also allow their customers in the public safety community to purchase compatible devices from their

competitors (Boyd Interview 2006). Proprietary standards lock consumers into buying from specific manufacturers in order to ensure compatibility with existing infrastructure. TIA, the organization contracted to develop the P25 standards, is primarily an organization that represents the radio manufacturing industry and was understandably caught in the middle. While it would be unfair to accuse manufacturers of trying to intentionally stymie progress, inherent conflicts of interest made the process long and difficult. As one commentator notes, "it is unrealistic to expect any business to wholeheartedly embrace a process that effectively destroys a valuable marketing tool" (Careless 2005). It was not until the federal government became involved that new interfaces began to be developed.

In 2004, NIST, and specifically its Office of Law Enforcement Standards, began to take a more involved role in the development of public safety communication standards. NIST began consulting with the P25 Steering Committee and helped it identify the three most important interfaces, besides the Common Air Interface, for enabling interoperability[21]. These interfaces were: the Inter-RF Subsystem Interface (ISSI), which uses internet protocol to link communication systems from different jurisdictions; the Fixed Station Interface, which defines how voice, data, and control messages are transmitted from fixed stations to mobile units; and the Console Interface, which describes how voice, data and control messages are transferred between mobile units and a dispatcher or supervisor.

[21] While all the interfaces in the P25 specifications contribute to interoperability in some way, some are more critical than others. For example, the Data Network Interface would only contribute to interoperability in limited situations when responders have the capability and need to access computer networks from the scene of an emergency.

NIST also offered the Steering Committee an interesting proposal. TIA had agreed to develop the P25 standards in the early 1990s, but there was nothing in the agreement that required the Steering Committee to adopt TIA's proposals. Through Congressional direction, NIST offered to create a set of intermediate standards for the Steering Committee, which would completely cut TIA out of the development process and would limit its control over future standard definitions (Orr Interview 2006). In an effort to retain control, TIA began to leverage its influence on industry to restart the standards development process. Realizing that the federal government would plunge ahead without its input, industry representatives agreed to increase their contribution to the standards process. Thus, due to NIST's involvement, the standards development process began to expeditiously move forward again.

As of May 2006, the ISSI is only weeks away from formalization and the other two priority interfaces should be completed and formalized by mid-to-late 2006 (Orr Interview 2006). Outside of NIST, federal support of the standards development process is being felt from both the legislative and executive branches of government. Congress has mandated P25 compliance on future radios being sold to the Department of Defense (Careless 2005) and the President's FY 2007 budget calls for changes to the "lack of shared technical standards... [that have] hampered the creation of regional communication systems that are interoperable" (Office of Management and Budget 2006). While there is still significant work to be done in developing and implementing P25 standards, the Steering Committee, the government, and industry are making positive progress towards comprehensive standards, going farther in the last 12 months than anyone has in the last 12 years.

Summary and a Look Ahead

The federal government has instituted a number of programs and policies to address interoperable communications, both in the near and long term. The intent of these actions is clear. Grant programs, technical evaluations, and special programs and initiatives will help public safety agencies purchase the equipment best suited to meet their needs. In conjunction with fostering collaboration between state and local agencies, these programs will help public safety agencies create at least limited interoperability in the immediate future. Spectrum and standards reform will have long-term results, because they will allow manufacturers to develop systems that are designed with interoperable functionality already in place.

However, while the intent is good, the effectiveness and timeliness of these programs is still in question. The next chapter will more carefully examine the policy decisions that were detailed in this chapter, and identify some concerns with our nation's ability to meet its interoperability goals.

References

AGILE. 2001. Operational Test Bed - Alexandria (OTB-A) Communications Interoperability Gateway Subsystem Operational Test Document. Rome, NY: National Institute of Justice.

Boyd, David. 2005a. United States Senate Committee on Commerce, Science, and Transportation. *Testimony of David Boyd, Ph.D.* September 29, 2005.

———. 2005b. U.S. House of Representatives Committee on Homeland Security - Subcommittee on Emergency Preparedness, Science and Technology. *Testimony of Dr. David Boyd.* October 26, 2005.

———. 2006. Personal Interview. Telephone, March 27, 2006.

Careless, James. 2005. What on earth is taking so long? *Mobile Radio Technology Magazine*, December 1, 2005.

Chandler, Nikki. 2003. PSWN Preparing to Shut Down. *Mobile Radio Technology Magazine*, June 1, 2003.

CommTech. 2006. *Operational Test Beds.* National Institute of Justice, 2006 [cited April 3 2006]. Available from http://www.ojp.usdoj.gov/nij/topics/commtech/testing_evaluation/.

Deficit Reduction Act. 2005. 109th Congress, Second Session, January 3, 2006.

Department of Homeland Security. 2004. *RapidCom 9/30 and Interoperability Progress*, July 22 2004 [cited February 20 2006]. Available from http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0470.xml.

———. 2005. Building Confidence in P25: Assessment Program Will Help Ensure Compliance. *Interoperability Today*, Summer 2005.

Doherty, Vin. 2006. Personal Interview. Washington D.C., March 29, 2006.

Gurss, Bob. 2006. Washington View - Promote Interoperability. *APCO International*, April 2006.

Intelligence Reform and Terrorism Prevention Act. 2004. 108-458. 108th Congress, Second Session.

Jenkins, William O., Jr. 2003. Homeland Security: Challenges in Achieving Interoperable Communications for First Responders. Washington DC: General Accounting Office.

Koontz, Linda D. 2004. Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration. Washington DC: General Accounting Office.

Levy, Leslie-Anne. 2006. Personal Interview. Washington DC, March 29, 2006.

Lipowicz, Alice. 2005. NIST, Safecom to validate first responder radios for interoperability. *Government Computer News*, 9/23/2005.

Manner, Jennifer. 2003. *Spectrum Wars: The Policy and Technology Debate.* Norwood, MA: Artech House.

National Task Force on Interoperability. 2005. Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives. Washington, DC: National Institute of Justice.

Office of Management and Budget. 2006. The Budget for Fiscal Year 2007: Department of Homeland Security, edited by Executive Office of the President.

Orr, Dereck. 2005. United States Senate Committee on Commerce, Science, and Transportation. *Testimony of Mr. Dereck Orr.* September 29, 2005.

———. 2006. Personal Interview. Washington DC, March 29, 2006.

Project 25 Steering Committee. 2006. *How was the P25 standard developed?* 2006 [cited April 13 2006]. Available from http://www.project25.org/Forum/misc.php?s=744bcdef18b52b3cb7670a872b0d2b8b&action=faq&page=4#five.

Project SAFECOM. 2005a. *Interoperability Continuum Brochure.* Department of Homeland Security 2005 [cited February 3 2006]. Available from http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1190_interoperabilitycontinuum.htm.

———. 2005b. Recommended Federal Grant Guidance: Public Safety Communications & Interoperability Grants: Department of Homeland Security.

———. 2006. *Frequently Asked Questions* 2006 [cited March 29 2006]. Available from http://www.safecomprogram.gov/SAFECOM/about/faq/.

Public Safety Wireless Advisory Committee. 1996. *Final Report of the Public Safety Wireless Advisory Committee to the FCC and NTIA*, September 11 1996 [cited April 10 2006]. Available from http://www.ntia.doc.gov/osmhome/pubsafe/PSWAC_AL.pdf.

Rudman, Warren B., Richard A. Clarke, and Jamie F. Metzl. 2003. Emergency Responders: Drastically Underfunded, Dangerously Unprepared. New York: Council on Foreign Relations.

Stevens, Ted. 2005. United States Senate Committee on Commerce, Science & Transportation. *Testimony of U.S. Senator Ted Stevens (R-AK)*. September 29, 2005.

Victory, Nancy J., Michael Lewis, Jr. Thomas S. Dombrowsky, and Catherine M. Hilke. 2005. Homeland Security and Communications: A Compendium of Federal Programs. Washington DC: Wiley Rein & Fielding LLP.

Chapter 4 – Federal Policy Analysis

The federal government has instituted a number of policies and programs to address a lack of first responder interoperability. NIST has promoted communication standards development, Congress and the FCC have pushed for increased emergency responder spectrum, and SAFECOM, within the Department of Homeland Security, has coordinated state and local government purchases of new equipment. Following September 11, the federal government has clearly taken action towards solving interoperability for emergency responders.

Despite these efforts, numerous critics have voiced concern that the federal response is not enough. The National League of Cities recently called on DHS to make "greater strides on interoperability," saying that the federal government was the only entity capable of solving many of the causes of noninteroperability (Drake 2006). In May 2006[22], the DHS Inspector General will be issuing a report that says DHS's Science and Technology directorate (S&T), which SAFECOM is a part of, is failing to live up to the interoperability mandates set out for it in the Homeland Security Act of 2002 (Skinner 2006). Perhaps the most damning criticism comes from the 9/11 Public Discourse Project, the public organization made up of the 9/11 Commission members. In their 2005 Report Card on 9/11 Commission recommendations, they gave the federal government a grade of C in its treatment of first responder interoperability issues (Kean, Hamilton, and et al. 2005). The Commission's Vice-Chairman, Congressman Lee Hamilton, recently lambasted federal response saying that "[it] really approaches scandal to think that four

[22] This report, *A Review of DHS' Progress in Adopting and Enforcing Equipment Standards for First Responders*, has not been publicly released as of this writing. It is, however, summarized in the Inspector General's Congressional testimony from March 8, 2006, and my summation is based on that testimony.

years after 9/11, the police and the fire cannot talk to one another at the scene of the disaster" (NBC News 2005).

The problem of interoperability is indeed complicated, and nobody who understands it expects an overnight fix. However, knowledgeable thinkers have raised legitimate concerns over the rate of progress in solving this problem. Thus, the two questions posed at the beginning of this thesis arise again: has the federal government made good policies towards emergency responder interoperability, and is the United States sufficiently positioned to finally solve this problem in a reasonable amount of time? These two questions will guide the analysis of the policies laid out in the previous chapters.

The Interoperability Budget

In order to gauge federal commitment to solving any problem, one should first look at how much money has been devoted to it. There are several estimates of the total amount of federal money that has gone to interoperability since 2001, ranging from around $1.5 billion to almost $3 billion. Because most of this money is in block grants, and the government generally does not track and itemize the types of equipment that local emergency responder grants are used for, an estimate is really the best one can hope for (Levy 2006). Careful inspection of the federal budget, however, paints a more detailed picture than the lump-sum value describes.

Interoperability has been a featured item in the homeland security budget since there first was a homeland security budget. Even before Congress created the Department of Homeland Security in 2003, the President's FY 2003 Protecting the Homeland budget

provided a side-box detailing the interoperability problems faced on September 11[23] (Office of Management and Budget 2002). The FY 2004 and FY 2006 budgets also mentioned interoperability, with the FY 2006 budget detailing the interoperability grant money that had been distributed through DHS during the previous year (Office of Management and Budget 2005). The FY 2007 budget goes so far as to identify a lack of "shared technical standards and coordinated operational plans" as one of the key impediments to interoperability (Office of Management and Budget 2006). Unfortunately, the President's submission to Congress is mostly explanatory and only breaks down the budget by departmental and directorate levels. It is up to the various Departments to determine how much money each program actually receives.

For the Department of Homeland Security, an organization that was only stood up in FY 2003[24], the budget data is unfortunately sparse. The DHS FY 2007 Performance Budget Overview[25] and the Budget in Brief list programmatic expenditures for the Office of Interoperability and Compatibility, with almost the entirety of this money going to SAFECOM. As Figure 4-1 shows, there was a massive increase in spending in FY05[26], followed by significant increases of 24% and 13% for FY06 and the FY07 request. These increases are much larger than the growth rate of the total DHS budget over that two year period, which has held steady at 7%. Less inspiring, however, is the fact that the total expenditure on interoperability programs in 2007 is only 0.08% of the total DHS budget

[23] The President's budget is generally submitted to Congress in the February prior to the Fiscal Year of that budget. The FY03 budget was submitted in early 2002, before the President was publicly supporting the idea of creating a Department of Homeland Security.
[24] The Fiscal Year starts October 1 of the preceding calendar year (i.e. FY 2006 started on October 1, 2005). The Department of Homeland Security was signed into law in November, 2002, stood up in March, 2003.
[25] The Performance Budget Overview (PBO) is a high level summary of program performance goals, performance measures, and budget information related to each program.
[26] The comparatively low $1.5 million outlay for 2004 is possibly a partial year value, that only includes money budgeted after the Office of Interoperability and Compatibility was created within DHS.

of $35.6 billion (Office of Management and Budget 2006). There are also only 14 full time DHS employees budgeted to work on interoperability programs in 2007 (Department of Homeland Security 2006).

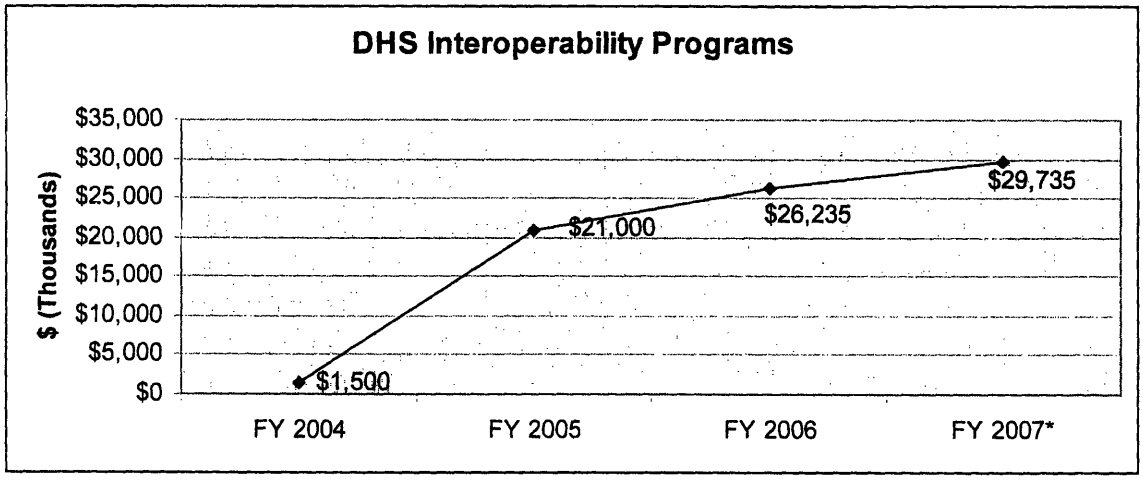

Figure 4-1 Programmatic Funding for Interoperability and Compatibility (FY 2007 is requested) Source: (Department of Homeland Security 2006)

The values in the above chart do not include grants that were distributed through DHS for interoperable communication at the state and local level. Homeland Security state and local interoperability grants come from the Office of Grants and Training (OG&T) within the DHS Preparedness Directorate. This office awards billions of dollars each year to state and local response agencies under a number of different grant titles. Unfortunately for analysis purposes, many of the grants are large block grants that serve a number of purposes, and OG&T does not categorize its grants by use. Therefore, there is no clear breakdown of how much DHS has doled out in interoperability grant money over the past few years. The director of SAFECOM estimates that, over the last three years, roughly half of the $2 billion in communication upgrade grants cited by OMB went specifically to increase interoperability (Boyd Interview 2006). He also notes that total

overall grants to state and local responders have been declining over that same time period.

Grant information is more detailed for the Department of Justice and its COPS Interoperability grant program. This program was started in 2003 to specifically provide grants for interoperability at the state and local level, and has since provided grants to 63 jurisdictions. As Figure 4-2 shows, funding levels in this program have been steadily on the rise. However, the amounts listed also show that only $386 million have been issued by the Department of Justice. This means that, regardless of the estimate for the total that one uses, the majority of federal interoperability grant money has come from DHS.

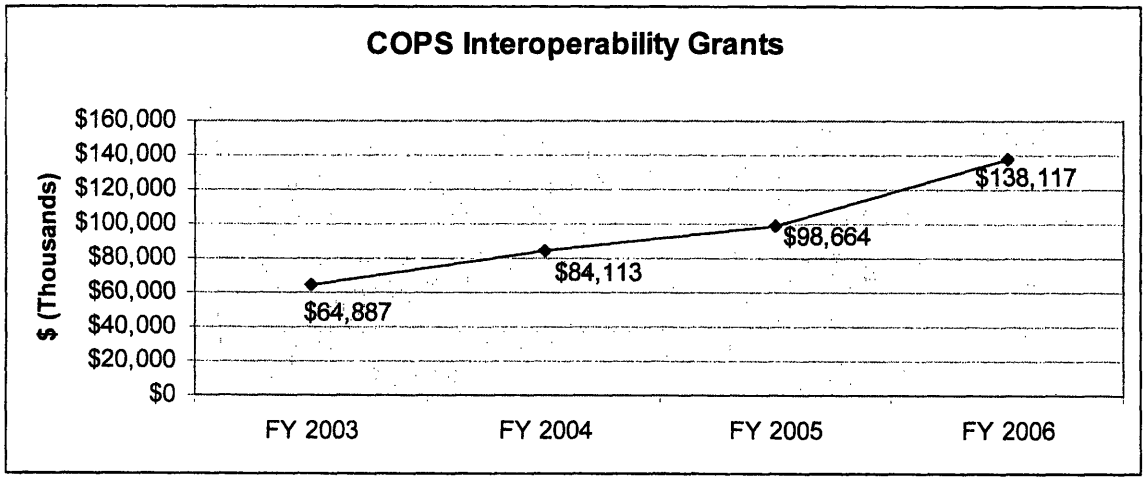

Figure 4-2 Grant funds for COPS Interoperability Grants
Source: (Department of Justice 2005)

With respect to COPS there are, surprisingly, no requested funds for FY 2007. That is because, for the third budget in a row, DOJ has attempted to eliminate the COPS Interoperability Grant program. DOJ argues that DHS should have sole authority over interoperability grants, but in each of the past two years, Congress has continued to fund the program at increasingly higher levels. This is largely because there is no dedicated interoperability grant program within DHS. Both the Association for Public-Safety

Communications Officials (APCO) International and the Democratic Staff of the House Committee on Homeland Security formally oppose the elimination of this program (Association for Public-Safety Communications Officials International 2006).

These quick peeks into the federal budgets show that spending on interoperable communications is growing at a much faster rate than other homeland security and first responder spending. Given cost estimates of $15-20 billion needed to fix the problem though and the lack of data on DHS grants, it is unclear if appropriations are increasing fast enough. It is also unclear what impact DOJ's elimination of COPS will have, if it actually goes through in the way that DOJ has proposed.

Organizing for Efficiency

The federal government has often been accused of duplicating efforts in its many departments and agencies. September 11 brought to light a number of duplicative efforts in the homeland and national security disciplines, from border control to disease prevention to interoperability. One of the major goals of the creation of the Department of Homeland Security in 2003 was to bring together the disparate and segmented security-related programs under one agency banner. In terms of interoperability, it was only partially successful with this.

Interoperability programs are still divided over four departments, with the majority concentrated in the Department of Homeland Security and the Department of Justice. SAFECOM coordinates these programs and tries to ensure that grants and projects are not unnecessarily duplicated, but it, of course, has no legislative authority to dictate the actions of DOJ or NIST programs. It also has no direct, sub-Cabinet way to compel its federal partners to provide agreed upon funding, should they decide to

withhold it. While SAFECOM's current leadership claims that the interagency collaboration has been operating smoothly in the past year (Boyd Interview 2006), this was not always the case. The programs early progress was impeded by both a lack of interagency agreements and interagency funding (Koontz 2004). If all interagency programs had been handled by the same federal department, SAFECOM would most likely have been more effective in its early days.

However, having multiple federal programs deal with interoperability does have some benefits. The fragmented approach allows individual offices to rely on core competencies that exist within their parent organization. For example, the Public Safety Communication Program (PSCP) at NIST benefits from the many NIST scientists and engineers who are experts at developing standards. If the PSCP were to be moved into some other department, such as DHS, its staff would be organizationally cut off from the technical expertise they rely on (Orr Interview 2006). The same is most likely true for the Department of Justice and the law enforcement expertise that it brings with it.

As stated in the budget discussion, DOJ is trying to eliminate the COPS Interoperability Grant program in FY07. If Congress approves this elimination, which they have blocked in the past two fiscal years, this would considerably reduce the size of DOJ's interoperability portfolio. This action would help streamline the grant application process for states and localities, as well as provide better oversight of interoperability grant awards because all grants would be distributed through DHS. However, it is essential that the money that would normally go to COPS gets transferred to DHS for interoperability-specific purposes. Otherwise, the federal government will be exchanging

millions of dollars in aide for a slight increase in efficiency. It is not yet clear if the COPS Interoperability Grant money will be deployed through DHS.

Purchasing Technology: Now vs. Later

The federal government has adopted a two-prong approach to addressing the interoperability problem. It helps states and localities purchase the technical solutions that are available now and provide limited interoperability, such as those discussed in Chapter 2. It also makes and implements policy decisions, such as developing standards and freeing spectrum, which will open the way for better technical solutions in the future. Unfortunately, the time factor involved presents federal, state and local decision makers with a classic dilemma: how does one maximize the usefulness of purchases in the present while not limiting their options in the future?

A hypothetical example may help illustrate the problem. Let us say that in 2007, the city of Orlando applies for an Urban Area Security Initiative grant that requests $200,000 for an additional six audio baseband switches. These devices allow messages from the Orlando Police Department and the Orlando Fire Department to be rebroadcasted on each others bands at the scene of an emergency. The city receives the grant, purchases and installs the devices, and then has limited interoperability[27] at the scene of an incident.

In 2009, competition between radio manufacturers drives down the price of a P25-compliant radio system to $2 million. Orlando applies for $1 million of new grant money and raises the same amount in matching funds. But because they already received $200,000 in interoperability funds just two years prior, they are cut from consideration

[27] As discussed in Chapter 2, baseband switches limit responders to only transmitting interoperable messages on a single channel, so they cannot use separate talking groups.

for the grant. Orlando policymakers begin to regret their decision to submit the grant for the additional baseband switches in the first place.

Almost all policymakers agree that interoperability is an immediate problem that should be fixed as quickly and as completely as possible. The inherent tradeoff between speed and completeness, though, should be cause for consideration by both federal grant managers and state and local response agencies. The effective use of grants is only part of the problem. In emerging technologies, there will always be some new technology just over the horizon. A new type of radio system, and its impact on public safety, should not be dismissed just because it is not fully developed and in place yet.

For those areas with no interoperability between response agencies, it is probably wise to apply for federal money immediately; a minimum level of interoperability is better than nothing. However, for areas simply wanting to expand the scope of their interoperable communications or link a new system into the network (i.e. bringing connections with the state police and the county sheriff online), it makes sense to at least spend time analyzing how current policy and technology directives will impact the interoperability landscape over the next 24 months. Purchasing immediately is not always the wisest course of action.

Spectrum and Standards: Impetus for Change

Both the push for standards and the release of spectrum to public safety officials have been delayed for years. P25 standards were first conceived of in 1989 and are only now being developed to provide network-level interoperability. Additional spectrum was authorized for public safety use in 1997, but Congress wrote the legislation in such a way that the TV stations occupying that spectrum would be allowed to sit there until 2007 at

the earliest. Only in early 2006 did they set an absolute date for the release of the spectrum. Even with the need for interoperability demonstrated by the Oklahoma City bombings, the Columbine High School shootings, and September 11, government officials failed to take action on these issues until 2005. Looking at the history, it is logical to wonder what took so long.

In the case of standards development, the government was simply not identified as a necessary player in the process until 2004. Before that, the P25 Steering Committee had contracted with TIA, a recognized Standards Development Organization, and was handling the process on its own. Although it was proceeding very slowly, the matter was being handled as a private-sector problem, without government interference. In 2003 and 2004, newly formed or redesigned government interoperability programs collectively identified a lack of standards as one of the major impediments to first responders. Based on recommendations by these groups, Congress started to take action and proposed "the issuance of intermediate standards," that would have taken the power away from private sector stakeholders and the TIA (*Departments of Commerce, Justice, and State Appropriation Bill of 2005* 2004). Before that, though, there was no push for any government agency to inject itself into the standards process.

As for spectrum policy, there was no argument about whether or not the government should be involved; no one else has the authority to allocate or regulate spectrum. This problem was more of a problem of shortsightedness on the part of Congress and the FCC. When Congress freed the 24 MHz of TV broadcast spectrum in 1997, they were operating under the assumptions that most TV stations would have already released control of the spectrum in question as they switched to digital

broadcasts. This conversion to digital is proceeding much slower than Congress anticipated, so the television stations continued to retain control of their spectrum.

Why Congress did not pass new spectrum legislation before Hurricane Katrina hit is still a mystery. The need for it was certainly there. In its 2004 report, the 9/11 Commission listed the release of spectrum as one of its chief recommendations (Kean, Hamilton, and et al. 2004). Numerous agencies alerted Congressional panels to the importance of spectrum. Bills that redefined the spectrum reallocation dates and deadlines were introduced, but were stalled or weakened in committee (Kruger and Moore 2005). The House started making serious efforts to pass spectrum reform in 2005, but it was only after Hurricane Katrina re-raised the problem of interoperability in the minds of the public that the Senate took up the issue. In early 2006, Congress finally passed legislation setting a fixed date for the transfer of spectrum. Public safety agencies in metropolitan areas can begin investing in equipment that uses that spectrum, confident, that it will eventually be available for them (Boyd Interview 2006). However, the date of February 17, 2009 is still so far in the future that it may make little difference for first responders who need extra spectrum now.

Federalism and Interoperability

This thesis has so far focused on the federal government's role in creating interoperability amongst state and local responders. However, the role of the states and localities themselves must not be forgotten. While the federal government has some obvious inherent advantages in its ability to set national policies and strategies for interoperability, the actual solving of the problem still occurs at the local level. It is local responders and officials who write the grant proposals for new equipment, raise the

matching funds through bond issues, develop partnerships with responders from neighboring jurisdictions, and determine how best to achieve interoperability in their community. Federal help is often appreciated, but it can be just as often rebuffed if it begins to intrude too much into the autonomy of the local agency. Thus, the problem of interoperability raises a much larger question that is found in many issues within the homeland security discipline: to what extent should the federal government involve itself in local preparedness decisions?

State and local emergency response agencies are designed to operate autonomously, without heavy federal intervention. The 10th Amendment of the Constitution says that those powers not expressly given to the federal government shall be retained by the states or the people. Thus empowered, these state and local governments set up response agencies that are uniquely suited to deal with the special challenges posed by the surrounding community. Generally, both the federal and the local governments agree that it is the localities that are best suited to determine and provide for their own needs. As one commentator puts it, "The people closest to the problem are the ones best equipped to find the best solution" (Carafano and Weitz 2006).

In terms of interoperability, however, there are a number of reasons why the federal government should be involved in the solution. First, federal agencies have enormous power to set and achieve broad goals, such as developing standards or reforming spectrum allocation. No single public safety agency or coalition of public safety agencies will ever be able to leverage as much power as the federal government in these arenas. Second, it has the ability to coordinate efforts between multiple stakeholders, and serve as a mediator when disputes arise. Building interoperability

requires that responders build consensus, and sometimes that requires the intervention of a third-party authority. Third, the government has the time and the expertise to think about broader issues of interoperability. In the majority of response agencies around the country, the responders are busy planning for and conducting day-to-day emergency operations. The federal government has the flexibility to sit back and evaluate equipment, look at proposed solutions, develop and share strategies, and serve as a central repository for interoperability knowledge. Fourth, interoperability is a problem that will require billions of dollars to solve. Barring significant investment by the private sector, the federal government is the only entity capable of relieving some of the economic pressure on the largely underfunded states and localities.

Interoperability conforms, in some ways, to a notion of a collective action problem. According to Mançur Olson, who first proposed this theory in the late 1960s, individual actors in a group that shares a common goal will not always pursue that goal, because doing so will result in the group gaining something with all the cost going to the individuals. In fact, Olson argues, "unless the number of individuals in a group is quite small, or unless there is coercion or some other special device to make individuals act in their common interest, *rational, self-interested individuals will not act to achieve their common or group interests*" (Olson 1971). A higher authority, such as the federal government, can be that "special device."

For example, all the response agencies in the state of Georgia might desire interoperability. A single town might consider lobbying for all agencies in the state to purchase new P25 compatible radio systems. But, the cost to that town to lobby for and coordinate a statewide upgrade makes it hard for the town to justify the effort. Only the

power of a broader authority can facilitate such action. While the Georgia state government could be the authority in this example, extrapolating this out to address a national problem of interoperability shows that federal involvement is most likely necessary.

A National Goal of Interoperability

The federal government has done many things to increase interoperability, but it has been unable to set a definable and measurable end goal. Without an end state in mind and a deadline for achieving it, there is no way to know if interoperability has been solved. As the Strategic IT Lead for the DHS Office of National Capital Region Coordination put it, "the interoperability train has already left the station, but it won't ever get to its destination" (Torres Interview 2006). There is no destination for that train to arrive at.

One of the reasons for this lack of an end goal is a problem of definition. Chapter 1 discussed how difficult it is to define interoperability, and how different response agencies at different levels of government expect different things from the term. SAFECOM has created its Statement of Requirements, which might be seen as a document that describes an end goal. But many of the listed requirements are broad and reach far beyond the basic interoperability notion of "responders being able to talk to each other." These requirements also try to combine the needs of every response agency imaginable, creating a set of functions that manufacturers would be hard pressed to provide.

But even if the Statement of Requirements is viewed as a reasonable end-state for interoperable technology, it does not lay out a timeframe for achieving interoperability or

specify what the nation can consider to be a success. There is no short, simply phrased, measurable interoperability goal. SAFECOM may eventually develop one, but as a small office in the federal government, it probably lacks the accountability to set a national imperative such as this. This problem deserves a goal to be set at the Cabinet or Presidential level, so that no one can question the national commitment to solving it.

Summary and a Look Ahead

In recent years, the federal government has been criticized for being sluggish and ineffective when dealing with interoperability problems. Some of these concerns are legitimate, but the landscape is changing. While both the legislative and executive branches were slow in responding to the need for standards and spectrum, they have recently made a large impact in these areas. Interoperability money has been increasing every year, and it has been doing so at a much faster rate than total homeland security expenditures. The end-state is still a mystery, and significant questions remain about how to best use money to achieve interoperability progress. But, despite this, incremental progress is being made.

The federal government is not the only national entity that has faced or is facing a lack of interoperable communications. Both the European Union and the United States military, among others, have dealt with similar interoperability issues. The next chapter will summarize these two cases to give comparative context to the federal government's approach.

References

Association for Public-Safety Communications Officials International. 2006. *Statement Regarding the President's Fiscal Year 2007 Budget Proposal*, February 13 2006 [cited April 10 2006]. Available from http://www.apcointl.org/government/positions/issuepapers/2007FederalBudget2-13-2006.pdf.

Boyd, David. 2006. Personal Interview. Telephone, March 27, 2006.

Carafano, James Jay, and Richard Weitz. 2006. Learning from Disaster: The Role of Federalism and the Importance of Grassroots Response. In *Backgrounder*. Washington DC: The Heritage Foundation.

Department of Homeland Security. 2006. Performance Budget Overview - Fiscal Year 2007, edited by Department of Homeland Security.

Department of Justice. 2005. FY 2006 Budget and Performance Summary, edited by Department of Justice.

Departments of Commerce, Justice, and State Appropriation Bill of 2005. 2004. 108-344. September 15, 2004.

Drake, Robert. 2006. Homeland Security Subcommittee on Emergency Preparedness, Science, and Technology. *Testimony of Mayor Robert Drake*. March 1, 2006.

Kean, Thomas, Lee Hamilton, and et al. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Company.

———. 2005. Final Report on 9/11 Commission Recommendations. Washington DC: 9/11 Public Discourse Project.

Koontz, Linda D. 2004. Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration. Washington DC: General Accounting Office.

Kruger, Lennard, and Linda Moore. 2005. The Digital TV Transition: A Brief Overview. Washington DC: Congressional Research Service.

Levy, Leslie-Anne. 2006. Personal Interview. Washington DC, March 29, 2006.

NBC News. 2005. *Transcript for December 4 - Meet the Press*. NBC News, December 4 2005 [cited March 15 2006]. Available from http://www.msnbc.msn.com/id/10266650/.

Office of Management and Budget. 2002. The Budget for Fiscal Year 2003: Protecting the Homeland, edited by Executive Office of the President.

———. 2005. The Budget for Fiscal Year 2006: Department of Homeland Security, edited by Executive Office of the President.

———. 2006. The Budget for Fiscal Year 2007: Department of Homeland Security, edited by Executive Office of the President.

Olson, Mançur. 1971. *The Logic of Collective Action*. Revised ed. Cambridge, MA: Harvard University Press.

Orr, Dereck. 2006. Personal Interview. Washington DC, March 29, 2006.

Project SAFECOM. 2006. *Frequently Asked Questions* 2006 [cited March 29 2006]. Available from http://www.safecomprogram.gov/SAFECOM/about/faq/.

Skinner, Richard. 2006. United States Senate Committee on Homeland Security and Governmental Affairs. *Statement of Richard L. Skinner*. March 8, 2006.

Torres, Nelson. 2006. Personal Interview. Telephone, March 31, 2006.

Chapter 5 – Interoperability within the European Union and the United States Military

The federal, state, and local emergency response agencies within the United States are not the only entities that deal with a lack of interoperability. Radio use is widespread among response agencies and militaries around the world, and most of these organizations have faced interoperability challenges of their own at one time. While the United States is still in the early stages of improving interoperability, other nations have progressed much further. Both the story of the European Union and the United States military serve as particularly interesting points of comparison to the United States' approach to solving the problem.

Interoperable Emergency Response in the EU

The European Union (EU) is an intergovernmental and supernational political body composed of 25 countries on the European continent. Member-nations share a common currency, a common fiscal and agriculture policy, and a common approach to a number of domestic and international issues. Because of the need for international support and response in a number of emergencies, the member-nations of the European Union have also taken a largely combined approach to ensure interoperability within their emergency response communities.

Interoperability first arose as a prominent issue for European responders in the late 1990s, around the same time that it did in the United States. While the tragedies of September 11, Oklahoma City and Columbine were geographically removed from the continent, Europe suffered its own share of disasters with responses that could have

benefited from interoperability[28]. Like the United States, European communities wanted to establish interoperability between agencies with overlapping jurisdictions and adjacent jurisdictions. Also like the U.S., European efforts were stymied by a lack of spectrum, standards, and funding. However, the European Union faced additional cross-national issues that the United States, as a single country, had never needed to deal with. European nations had historically had the autonomy and authority to establish their own frequencies and communication policies. Before the late 1980s, there were no regulatory bodies, like the FCC or NIST, which could create Europe-wide policies and standards for communication equipment (Worrall 2005). Thus, achieving interoperability between responders from different countries involved a shuffling of historically national regulatory systems, and would seem to be much harder than achieving interoperability between responders from different American states, regions, and levels of government.

Despite the additional roadblocks posed by international coordination within the EU, scholars believe that "Europe quickly overtook the United States in the march towards interoperability" (Mayer-Schönberger 2002). Europe has established a plan towards interoperability that is based on three things: a quick adoption of standards, the use of a standards-dependent frequency framework, and innovative methods to encourage private investment in public infrastructure. While there is no guarantee that implementation of this plan will result in the EU achieving better interoperability more

[28] A principle example of an interoperability-related disaster was the February 1999 evacuation of the town of Galtuer, Austria. Three avalanches had slammed down on the winter ski village, killing 31, cutting power to the town, and blocking the only way out for the roughly 17,500 tourists and residents. Multiple agencies brought rescue helicopters in to evacuate the population, but these helicopters were unable to communicate. Alpine gendarmes had to distribute their old radio systems to the helicopter pilots, and, over a series of days, these single-channel systems were the only resource available to coordinate a massive rescue effort (Mayer-Schönberger 2002).

quickly than the U.S., their approach has given them what appears to be a significant advantage adopting interoperable policies (Mayer-Schönberger 2005).

The first part of the European Union's interoperability strategy was the development of standards for communication. Like the development of radio standards in the United States, development in Europe started in the late 1980s[29]. The newly created European Telecommunications Standards Institute (ETSI) was charged with creating a set of radio standards that would be usable by a number of sectors including public safety, transportation, public utilities, and industry. The result, TETRA, was a set of open, non-proprietary standards for digital trunked radio communications that purportedly allowed interoperability between all radio users, not just the public safety community (TETRA MoU Association 2006a). Like Project 25, TETRA defined eight interfaces for air, console, and network communications[30]. However, all eight of TETRA's interfaces were finalized in the mid-1990s with first generation devices and networks deployed in 1997 (TETRA MoU Association 2006b). As discussed in Chapter 3, the United States' Project 25 is still in development and will only have three of its eight interfaces defined by 2007.

TETRA has now become the dominant radio communication standard in Europe, with almost 90 manufacturers building systems that incorporate the open interfaces. TETRA is also starting to see limited use in South America, Africa, the Middle East, and China (TETRA MoU Association 2006a). Some manufacturers have considered marketing it in the United States, but intellectual property restrictions have kept it from being allowed in North America (Mohney 2005). Still, with over 4 million users expected

[29] European communication standards were first being developed as the European Union, itself, was being formalized as a political body.
[30] The eight P25 interfaces and the eight TETRA interfaces are named and defined differently. However, several interfaces from each set have functionally equivalent interfaces in the other.

in the next three years and inroads being made into expanding worldwide markets, TETRA is viewed as a wildly successful set of standards (Mohney 2005).

There are several reasons why TETRA's development and adoption may have occurred faster than that of P25 in the United States. First, it had widespread EU support early in its development. Mayer-Schönberger suggests that EU officials were willing to get involved in the standards process at an earlier stage than the US government, because Europe had already seen the success of a government-selected standard for cellular phone networks[31]. Thus, the idea of promoting radiocommunications standards was not foreign to European policy makers (Mayer-Schönberger 2005). Second, TETRA was designed to be usable in a number of sectors, not just public safety. With more private investors and commercial stakeholders interested in its successful completion, there was more pressure to get it completed and finalized. Finally, TETRA was closely linked with a spectrum reallocation plan for emergency responders. The European Radiocommunications Committee[32] (ERC) mandated that users would need to switch over to TETRA-based systems if they wanted to use the increased spectrum (*ERC Decision of 7 March 1996 on the harmonised frequency band* 1996).

The second component of the EU's approach to interoperability was a spectrum reallocation that was tightly coupled with standards. TETRA standards were designed and optimized for additional spectrum that would be released to mobile radio users. In 1996, the ERC designated 10 MHz of spectrum as TETRA-only, and they rolled out an

[31] The European Union passed legislation mandating that all European countries must use cell phone networks based on the GSM standard. The United States opted for market-defined standards and now plays host to two competing cell phone networks: GSM and cdmaOne.

[32] The European Radiocommunications Committee, formed in 1991, was the radio regulatory body of the European Union. The ERC performed duties that are filled by both NIST and the FCC in the United States. In 2001, the ERC was merged with the European Committee for Telecommunications Regulatory Affairs to form the Electronic Communication Committee. For more information, see http://www.ero.dk/.

additional 10 MHz before the year 2000 (Mayer-Schönberger 2002). Unlike the FCC in the United States, directives from the ERC are non-binding and require ratification by each nation. However, by 2001, twenty-six European countries had abided by the ERC decision and released the TETRA-only frequencies for emergency responders and others[33] (Mayer-Schönberger 2002).

The third part of the European approach to interoperability, funding, was also strongly integrated with TETRA. Digital-trunked radio systems like TETRA require significant infrastructure investment, especially when they replace aging and incompatible analog systems (National Law Enforcement and Corrections Technology Center 2003). In order to fund this infrastructure, many nations opted for a public safety/public service cost sharing program that prioritized emergency responder transmissions over the transmissions of other public service agencies (i.e. local government, sanitation, etc.). In the UK, the government opened competitive bidding for a private company to build and maintain the communications infrastructure. British Telecom won the bid, and capitalized on a unique market opportunity by charging public safety and service agencies to use its TETRA network (Mayer-Schönberger 2005). In this way, the cost of the infrastructure replacement was absorbed by the commercial entity as investment on a future business opportunity. In such a scheme, public safety agencies are still responsible for purchasing their radios. However, the open, non-proprietary standards of TETRA allowed the roughly 90 manufacturers in the sector to be in competition with each other, which drove down unit prices (Mohney 2005). National subsidies also helped defray the cost to response agencies (Mayer-Schönberger 2005).

[33] France and the Czech Republic opted against the use of TETRA and instead developed a completely independent and incompatible system called TETRAPOL.

TETRA-based systems are widely used around the world and have a number of inherent benefits. However, critics are quick to point out that TETRA is not the end-all solution for first responder interoperability. First, the fact that it is not targeted directly at first responders, like P25 is, means that some features first responders require may not have been adequately addressed. For example, responders are generally uncomfortable with sharing a network, because of the risk that it might become overloaded by civilian traffic during an emergency (Doherty Interview 2006). Don Pfhol, director of the Project 25 Steering Committee, also points out that TETRA radio signals do not transmit as well as P25-based signals do over long distances. Because of this, most TETRA networks would require too many towers to be economical in rural areas. By Pfhol's estimate, "in ninety percent of the United States... you don't have the population density to justify anything but Project 25" (Mohney 2005).

Because European and American interoperability policies were developed during roughly the same timeframe, most of the lessons from Europe do not transfer easily to the United States. The U.S. is already starting to engage standards and spectrum issues in a more heavy-handed way that is reminiscent of the EU's approach. One area that the United States would benefit from exploring is the potential for public-private partnerships in the funding of emergency network infrastructure. Once P25 standards are well-defined, the leasing of privately owned networks could provide new avenues for interoperability that do not rely exclusively on tax dollars.

Interservice Interoperability in the U.S. Military

In 1983, the United States invaded the island nation of Grenada in order to quell a communist uprising. During that military operation, multiple press reports detailed the

inability of officers from one branch of the service to communicate with members of the other services. In one striking example, "it was reported that one member of the invasion force placed a long distance, commercial telephone call to Fort Bragg, N.C., to obtain C-130 gunship support for his unit which was under fire" (Anno and Einspahr 1988). These reports prompted the Department of Defense to seriously examine the state of their Command, Control, and Communications Interoperability (C3I)[34] between the services.

One might assume that the Department of Defense would have a much easier time achieving interoperability than the public safety community. The Department of Defense is much more hierarchical than the autonomous fire and police departments and other first responder agencies across the nation. The Department also has significant control over its allotted spectrum and significant financial resources to procure new technology. While interservice rivalries do exist, very few military officers doubt that interoperability would help them conduct their missions. Despite these obvious advantages, however, a lack of interoperability is a problem that plagued almost every major military operation in the 1990s, from Desert Storm to Kosovo (Faughn 2002). Even now, when officers can communicate outside their services in most situations, there are still examples of interoperability shortcomings in current operations in Iraq and Afghanistan (Pickup 2005). The state of military interoperability is much better than it was in 1983, but there is still work to do to ensure full compliance.

In confronting interoperability issues, the military faced many of the same challenges that the public sector now faces. In World War II, the military was

[34] Interoperability in the military is generally defined much more broadly than interoperability for public safety agencies. While first responders are mostly concerned with being able to talk to each other, military systems must transmit location and tactical data, video, and other telemetry that extends beyond first responder needs. This discussion will try to stay focused on the ability to talk between services via radios. Also, C3I is now frequently referred to as C4I because of the addition of Computers.

surprisingly interoperable because all the communication systems in use were purchased around the same time and from the same vendor (Faughn 2002). However, in the 50 year military buildup following that war, new communication systems replaced the old ones without taking interservice communication into account. According to a 1999 report by the National Research Council,

> "The military services have tended to retain legacy information systems that were developed in response to "stand-alone" requirements, were not regarded as subject to connection with other systems and, therefore, are not operationally friendly with their increasingly interdependent companion systems. The legacy systems issue is one of the greatest challenges faced by the DOD today" (Committee to Review DOD C4I Plans and Programs 1999).

The military also suffered standardization issues similar to those faced by public safety agencies. As the military shifted its buying patterns towards commercial off-the-shelf technology for communications, it acquired many of the same proprietary protocol conflicts that prevent first responders from talking (Faughn 2002). Finally, although the defense budget is orders of magnitudes larger than public safety budgets, it is not unlimited. There are still problems funding new communication equipment, especially when it is prioritized against the various other weapon and warfighting needs of the military (Committee to Review DOD C4I Plans and Programs 1999).

Some of the military's interoperability problems were also decidedly unique. For example, at the end of the Cold War, some weapon systems that were intended to fight the nuclear threat were given conventional military roles[35]. Communication systems in these platforms were never intended to be interoperable with ground troops (Faughn 2002), so in order to make them effective in conventional operations, these communication systems had to be upgraded or replaced. In recent years, the U.S. military

[35] The B1 Bomber is a good example of a Cold War weapons platform that was given a new role as a tactical bomber.

has also conducted numerous operations as part of a larger coalition. Creating trans-national interoperability between coalition units is especially challenging, because the entire technical frameworks of the systems are often different (Illingworth 2002).

The military's approach to achieving interservice interoperability is a combination of procurement policies, organizational changes, and directives from on-high. As early as 1967, the DoD issued an interoperability directive saying that military departments should develop and procure compatible C3 equipment as a matter of policy[36]. According to the GAO, however, "the [directive] was not adequately implemented,... nor was it revised in a timely manner to provide necessary authority" (Conahan 1987). Disagreements between the services prevented amendments to the directive until 1985, when the Senate Armed Services Committee threatened to withhold all funds for communication equipment unless the policy was updated (Conahan 1987). Since then, the policy has been updated on a fairly regular basis, as new interoperability requirements arise[37]. According to some, however, services still occasionally procure non-compliant and non-interoperable communication equipment (Faughn 2002).

The Department of Defense also instituted numerous organizational changes that helped promote interoperability. One of the most critical changes was the Goldwater-Nichols Act of 1986. This law prompted an almost complete overhaul of the DoD, centralizing power with the Secretary of Defense and positioning the Chairman of the Joint Chiefs of Staff as the principal military advisor to the President. The Act also moved much of the power away from the service chiefs (i.e. the Army or Navy Chief of Staff), which made it much easier to promote interservice collaboration and

[36] DoD Directive 4630.5, originally issued on January 28, 1967.
[37] The latest version of the Directive, dated May 5, 2004, can be found at http://www.dtic.mil/whs/directives/corres/pdf2/d46305p.pdf

interoperability (Illingworth 2002). Although it was not specifically directed at communication interoperability, Goldwater-Nichols changed the way that services worked together and was a critical step in making interoperability a logical requirement for the officer corps.

Over the past 25 years, there have been numerous programs aimed at creating interoperability. The Joint Interoperability for Tactical Command and Control Systems (JINTACCS) program defined message standards and interfaces for C3I during the early 1980s. The TRI-TAC program developed fieldable telephone switches and radios for deployment, and looked at broader issues of interservice communication. The Joint Tactical C3 Agency provided oversight and management of interoperability operations throughout DoD (Conahan 1987). In the 1990s, the limited success of the programmatic approach prompted the Department of Defense to adopt an "interoperability triad." This triad consisted of an operational architecture, a systems architecture, and a technical architecture that were developed in concert and were meant to define overarching strategies for interoperability (Committee to Review DOD C4I Plans and Programs 1999). As technology changed, oversight programs were put in place to make sure that newly acquired technology met interoperability plans and guidelines (Faughn 2002). In short, no one program, plan or strategy got the military to its current state of interservice interoperability. It required a number of programmatic changes, strategic directives, and organizational overhauls to apply a fix to the problem, imperfect though that fix may be.

If the U.S. military story is a good approximation of the emergency responder story, then there is a long road ahead before this nation's public safety agencies can truly achieve interoperability. Grenada was the military's September 11 – an event where the

lack of interoperability was brought to light in a very public way. Yet, more than twenty years after Grenada, interoperability between the services is still not perfect. To even get to their current level of interoperability, the military had to try a number of approaches and strategies, and institute a new organizational framework for the entire Department of Defense. The thousands of emergency response agencies in this country lack the centralized command structure, massive budget, and other advantages that DoD has when dealing with interoperability issues. It may be foolhardy to expect that they can achieve interoperability any faster than the military.

Summary

The European Union and the United States military both present intriguing comparisons to the interoperability activities of the U.S. federal government. All three organizational entities have faced or are facing similar technical challenges, yet each is approaching them differently. The U.S. military is by far the farthest along in achieving full interoperability, but it started working towards it more than 15 years earlier than the EU or the U.S. public safety community. Despite its hierarchical command and control structure, it had to try numerous policies programs to make headway. The European Union, on the other hand, is moving the quickest towards interoperability, by building their entire policy around a single set of standards – TETRA. All though this approach so far seems successful, putting all its resources towards one technology may limit the EU's options in the future. The United States federal government is taking a middle of the road approach, with a few decentralized programs that are coordinated through a single office. However, it remains to be seen if the United States public safety community can ever achieve more than incremental progress towards interoperability.

References

Anno, Stephen E., and William E. Einspahr. 1988. The Grenada Invasion. In *Command and Control and Communications: Lessons Learned.* Maxwell Air Force Base, AL: Air University Press.

Committee to Review DOD C4I Plans and Programs. 1999. Realizing the Potential of C4I: Fundamental Challenges. Washington DC: National Research Council.

Conahan, Frank C. 1987. Interoperability: DOD's Efforts to Achieve Interoperability Among C3 Systems. Washington DC: General Accounting Office.

Doherty, Vin. 2006. Personal Interview. Washington D.C., March 29, 2006.

ERC Decision of 7 March 1996 on the harmonised frequency band to be designated for the introduction of the Digital Land Mobile System for the Emergency Services. ERC/DEC/(96)01. March 7.

Faughn, Anthony W. 2002. Interoperability: Is it achievable? Cambridge, MA: Center for Information Policy Research - Harvard University.

Illingworth, Gary. 2002. Command, Control (C^2) and Coalition Interoperability Post '911': Introducing the Network Centric Infrastructure for Command Control and Intelligence. Rome, NY: C3I Associates.

Mayer-Schönberger, Viktor. 2002. Emergency Communications: The Quest for Interoperability in the United States and Europe. *International Journal of Communications Law and Policy* (7).

———. 2005. The politics of public safety communication interoperability regulation. *Telecommunications Policy* 29:831-842.

Mohney, Doug. 2005. Is this finally P25's year? *Mobile Radio Technology*, May 1, 2005.

National Law Enforcement and Corrections Technology Center. 2003. Guide to Radio Communications Interoperability Strategies and Products. Rome, NY: AGILE Program.

Pickup, Sharon. 2005. Unmanned Aircraft Systems: DOD Needs to More Effectively Promote Interoperability and Improve Performance Assessments. Washington DC: General Accounting Office.

TETRA MoU Association. 2006a. *About TETRA>First Time Visitor* 2006 [cited April 23 2006]. Available from http://www.tetramou.com/tetramou.aspx?&id=1192

———. 2006b. *Why TETRA>TETRA Standard* 2006 [cited April 18 2006]. Available from http://www.tetramou.com/tetramou.aspx?&id=2229

Worrall, Steve. 2005. An International Study of Radio Interoperability, Rushmore University.

Chapter 6 – Charting a Path Forward

The introduction to this thesis contained two key questions. First, has the federal government implemented good policies towards achieving interoperability between first responders? The answer, as detailed in the previous chapters, is a qualified yes. Though slow to start, the federal government has made progress in developing standards, freeing spectrum, and funding the purchase of new equipment. They are beginning to evaluate equipment and implement stop-gap solutions in risk-prone cities. Funding levels have not yet reached what most would consider an adequate level, but federal funding is on the rise. While more money or man-hours would be useful to solving the problem, the federal government is satisfactorily fulfilling its role of supporting state and local response agencies. Incremental progress is being made towards interoperability.

The second question – is the United States sufficiently positioned to solve interoperability in a reasonable amount of time – is, of course, hard to answer. First, no one really knows what "solving interoperability" looks like. It is easy to suggest that buying new standards-based radio systems that operate in the right spectrum range will solve interoperability. Yet even with all the technical advantages and money in the world, public safety agencies will not be interoperable without a governance structure, joint exercises, and adequate training and support. If public safety agencies plan and train together, they might only have interoperability during the trained for emergencies and not during the unanticipated encounters. Interoperability may never be something that can be solved – it can just get successively better.

In this second question, a "reasonable amount of time" is also an unknown quantity. Some experts estimate that it will take another 15 years before the U.S. achieves a pervasive level of interoperability. If the military example is any indication, such estimates might very well be accurate. When asking about a timeframe, what policymakers really want to know is, "Will a lack of interoperability ever again impede the response to a major disaster?" Unfortunately, the answer is probably yes. No matter how good the nation's cross-agency communications get in the next few years, there will still be places that both lack interoperability and are vulnerable to disaster. If future terrorist attacks, natural disaster, or large-scale criminal events occur in these places, they will most likely suffer from an inadequate response that is caused, in part, by a lack of interoperability.

The irony of this is that disasters that are worsened by a lack of interoperability are the best catalysts for ensuring that interoperability continues to improve. September 11 prompted the creation of SAFECOM and the reorganization of interoperability efforts within the federal government. Hurricane Katrina prompted Congress to set a hard date for the release of spectrum to first responders. The regular occurrence of such disasters keeps the funding for interoperability programs increasing. Conversely, if the next disaster occurs in a place where partial interoperability has been achieved, there is the possibility that funding for interoperability programs will be cut, because the problem is already shown to be "solved."

The federal government has made a good start at creating incremental improvements towards interoperability. There are still, however, many more actions that

they can and should take. The following recommendations are designed to provide a path forward for federal involvement in interoperability.

Recommendation 1: Encourage better collaboration between local agencies by hosting roundtable discussions

SAFECOM should host roundtable discussions in those communities that lack memorandums of understanding or governance agreements. The purpose of these discussions will be establishing a timeframe in which to develop those agreements.

Collaboration is one of the most important, yet most frequently ignored, needs when discussing interoperability. If responders have not met each other, trained together, and hammered out command and control issues before a disaster, the fact that they can talk to each other during a disaster will be meaningless. Collaboration can also help response agencies coordinate purchasing plans and make the purchasing decisions that best fulfill the combined goals.

The first step in any collaborative effort is a meeting where goals, objectives, and timeframes can be discussed. SAFECOM should establish these initial meetings in communities where interoperability has not yet been addressed at a procedural or organizational level. In order to conduct and facilitate these meetings, SAFECOM should hire between two and four "evangelists" who will arrange these discussions. These so-called evangelists will facilitate the meeting, help convince the stakeholders of the need for interoperability, and guide the participants towards establishing a timeline for the development of governance agreements. Evangelists will also help participants understand the federal role in building interoperability.

Recommendation 2: Encourage better industry participation through endorsements and public/private partnerships

The Department of Homeland Security should push for the creation of an independent review panel for new public safety communication systems. This panel should give endorsements to those communication systems that perform well, promote interoperability, and have compelling feature sets. These endorsements should be communicated to the public safety consumers who are looking at buying these systems. SAFECOM should also establish a pilot program that promotes the use of a privately owned, publicly used communication network.

The private sector has been poorly engaged in the efforts to achieve interoperability. The federal government has been reluctant to intrude in to the workings of the market, and the market has been slow in responding to responder demands for open standards. Now that open standards are becoming a reality, the federal government must encourage the private sector to be more closely aligned with the goals of its public safety agency consumers.

The first step is to ensure that the private sector is producing products that meet emergency responder needs. SAFECOM and NIST, in a positive first step, are establishing a program that will evaluate new products to ensure that they are Project 25 compatible. However, emergency responders face a number of choices when choosing a communication systems vendor. Even if something is P25 compatible, it may not have good coverage, easy of use, or otherwise fulfill responder needs. To help public safety agencies make the best choice regarding their purchases, the Department of Homeland Security should push for the creation of an independent review panel. This review panel should evaluate new systems on a number of different metrics and include an endorsement system that gives a "Seal of Approval" or "Editor's Choice"-type award to deserving products. This endorsement would be highly sought after by manufacturers, because it would instantly highlight their products for their consumers. Qualification for

this endorsement would be based primarily on the ability of the system to be interoperable, but it would also include ease of use, price, and the system's feature set. Grant proposals that include the purchase of endorsed systems might also be given greater consideration in the competitive process, although this could produce the unintended consequence of localities proposing purchases that do not fit their needs, just to win the grant.

Besides promoting an endorsement system that is aimed at encouraging manufacturers to produce better products, the Department of Homeland Security should institute a pilot program that encourages public/private partnerships on investments in communication networks. As Chapter 5 discussed, Great Britain created an excellent private-sector opportunity when British Telecom invested in new communication infrastructure and then charged responders a monthly fee to use it. Such a program could easily be repeated in the United States, although it would have to be in a region of the country that is both looking to upgrade its communication systems and has enough responder density to justify the cost model. The federal government will participate by bringing the stakeholders to the table and, if necessary, providing a buyout option for the private firm, should the pilot program fail.

These are just two examples of ways in which public and private interests can align through federal action. By encouraging further private sector involvement in interoperability through other novel solutions, the government can help increase the speed at which interoperability becomes pervasive in our nation.

Recommendation 3: Create an interoperability grant program within DHS

The Department of Homeland Security's Office of Grants and Training should establish a new grant program that provides money to exclusively increase interoperable communications. Under this new structure, states and localities would no longer be allowed to apply for interoperability equipment through block grants or DOJ interoperability grants. Instead they would apply directly to this new program.

As discussed in Chapters 3 and 4, there is no grant program within DHS that is specifically designed to provide money for interoperable communications. Instead, state and local agencies can apply to a number of different general or block grants and include interoperability as a component of those applications. The Department of Justice has the COPS Interoperability Grant program, which does provide money exclusively for interoperability, but OMB has repeatedly tried to eliminate that program. If they are successful, there will be no specifically institutionalized support of interoperability within the federal government.

Creating an interoperability grant program as the exclusive source of federal interoperability funds will serve a number of purposes. First, it will ensure that funds that could go to this problem are not lost to serve other, less important, homeland security initiatives. There are numerous stories – some probably apocryphal, but still relevant – of small towns using homeland security grants to purchase unnecessary video cameras, SUVs, and air conditioned garbage trucks. While the localities are in the best position to determine their own needs, and most homeland security money does go to fix real first responder problems, interoperability deserves special attention as a problem that affects almost all public safety agencies. Removing interoperability funding from general homeland security grants will ensure that the localities with real interoperability needs will not be in competition with those whose needs may be less immediate.

A separate interoperability grant within DHS would also placate critics who are upset that the COPS Interoperability Grant program is being phased out. Critics are worried that the phase-out will reduce the visibility of interoperability as a national problem. They are also worried that once the program is eliminated, the money that would go into it will be reabsorbed by the Justice Department and not appropriately distributed to first responders. The new interoperability grant would condense the majority of interoperability programs within DHS, keep interoperability at a high level of collective consciousness, and provide transparency for the budget walkover between DOJ and DHS.

Finally, this grant program will provide much more data about the amount of federal money that is going to fix interoperability. Financial estimations are not sufficient when dealing with a problem of this importance. While a careful review by auditors would be able to calculate the exact amount of federal money that is going towards interoperability, a budget line item would be a much more easily obtainable data source that would provide valuable information to the first responder community, Congress, and the public. Such a program would also make it easier for outsiders to determine which areas are improving their ability to communicate. Interested parties could then track the outcome of interoperability grant money and determine if the millions of dollars spent each year are having any real impact.

Recommendation 4: Prepare now for a large increase in interoperability funding once systems based on new standards and spectrum become available in 2009

The Department of Homeland Security and Congress should recognize that the completion of the Project 25 open standards, in concert with the release of new spectrum in 2009, will constitute a technological leap forward for interoperable communications. In the 2008 and 2009 budget, DHS should increase money for interoperability grants by at least 25%.

As discussed in Chapter 3, Project 25 radios are currently available, but they only implement one of the eight interfaces in the P25 standards suite. The other three critical interfaces for interoperability will be finalized by the end of 2007. Systems that implement these four key interfaces should be available for purchase in mid-2008 and early 2009, right around the time that the 24 MHz of allocated spectrum will be released for first responder use. A lack of spectrum and a lack of standards are the two remaining major technical barriers to interoperability, and the release of this new technology will overcome both of them. Therefore, many public safety agencies will want to upgrade their communication systems to P25 systems that use the newly available spectrum. The federal government must be prepared to accommodate a surge in funding requests.

In order to adequately meet the increased demand for federal aid, DHS should prepare to fund an increased number of interoperability grants to state and local responders in the 2008 and 2009 budgets. Considering that this increase will occur during the first year of a new presidential administration, Congress will be more likely to approve additional appropriations, especially if interoperability becomes an issue in the 2008 elections. Barring that, this money will have to come from other grant programs within the Department of Homeland Security. While transferring money will always

necessitate security tradeoffs, interoperability should take funding priority because of the unique opportunities posed by the convergent timing of these two technical advances.

Recommendation 5: Establish a National Interoperability Goal

The President of the United States should announce a national interoperability goal that sets a specific deadline for a measurable result. One possible goal that is both logical and feasible is, "By the year 2010, every public safety agency that operates in a region on the Urban Areas Security Initiative list will have incident command-level voice communication with every other public safety agency – local, county, state, tribal and federal – that operates in that region."

The policies, activities, and dollars of the federal government are increasing regional interoperability in pockets and spurts. In order to have true national progress, though, there needs to be a big, long term, audacious national goal. This goal should be simple, easy to understand, and should clearly state what the national policy on achieving interoperability will be and how the nation will know if it's been achieved or not. The details can continue to be handled as they have been for the past few years, but the overarching vision must be made anew. In short, interoperability needs a statement akin to President Kennedy's famous "We choose to go to the moon" speech, in which the President set both a big, audacious goal and a short timeline with which to achieve it.

The statement proposed above is not the one that has to be used, but it is a good starting point for a number of reasons. First, it sets a clear and relatively tight timeline for the goal to be achieved. With only 3.5 years until 2010 at the time of this writing, there is enough pressure to make all levels of government address this now. Second, it defines the set of regions it is looking at as those on the Urban Area Security Initiatives list. This list, complied by the Department of Homeland Security, identifies the most sizable or risk-prone cities in the nation. While interoperability is not just a homeland security-related

problem, it is the fear of future terrorist attacks and natural disasters that will motivate this effort. Finally, the statement describes exactly what must be achieved. Every public safety agency, from firefighters to local police to paramedics to the state police and National Guard, needs to be involved. The communication must at least exist between the incident commanders from each agency at the scene, much as it was in the RapidCom pilot that was detailed in Chapter 3.

Achieving this goal will not be easy, nor will it ultimately be an end-state for interoperability. Cities not on that list will still need interoperable communications, and even the regions that are addressed will need more comprehensive interoperability. But as this goal is achieved, a new one can be set and pursued. In this way, the quest for national interoperability will be constantly overcoming remaining obstacles, driven towards ideals, and following a path forward.